GUIDE MISE EN CONFORMITÉ R.G.P.D.
EN 4 ÉTAPES

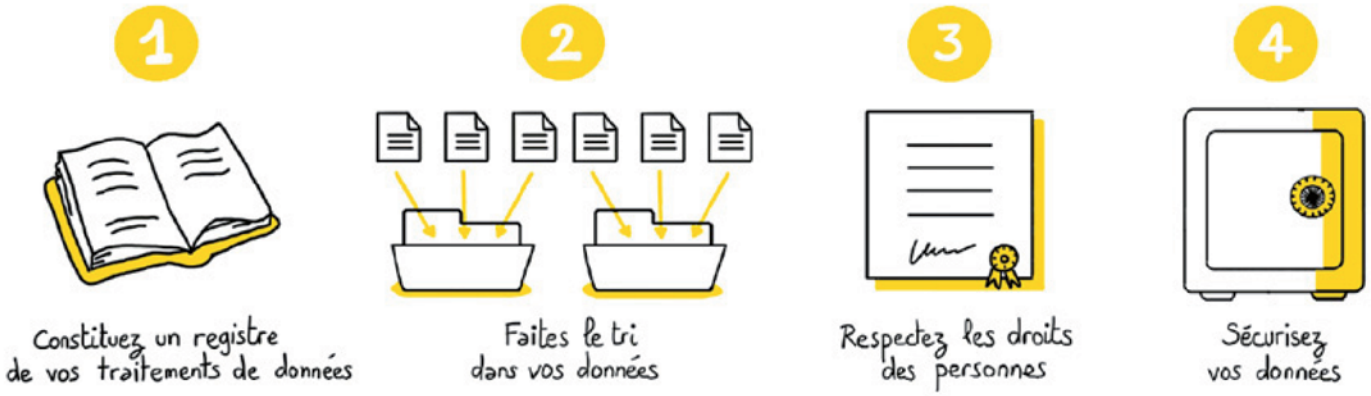
R.G.P.D. Réglement général sur la protection des données

cnatp
Les artisans des Travaux Publics et du Paysage
Haute-Vienne

CAPEB
L'Artisanat du Bâtiment
HAUTE-VIENNE

MON CHOIX, MA RÉUSSITE

PASSEZ À L'ACTION EN 4 ÉTAPES



1 - REGISTRE DE VOS TRAITEMENTS DE DONNÉES

Complétez le Registre de traitement de vos données (1) et créez une fiche pour chaque activité recensée, en précisant :

- l'objectif poursuivi (exemple : fidélisation client) ;
- les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, etc.) ;
- qui a accès aux données (exemple : service commercial, direction, prestataires, partenaires) ;
- la durée de conservation de ces données.

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

Vous n'avez pas en revanche à mentionner au registre les traitements purement occasionnels (exemple : fichier constitué pour une opération événementielle ponctuelle comme l'inauguration d'une boutique).

(1) Modèle fourni disponible auprès de la CAPEB 87

2 - FAITES LE TRI DANS VOS DONNÉES

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 (2) »** 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.**

Quelques exemples de durée de conservation :
- 3 ans : données de vos clients utilisées à des fins de prospection commerciale à compter de la fin de la relation commerciale. Au terme de ce délai, vous pouvez reprendre contact afin de savoir si votre client souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées.
- données des salariés : 5 ans (en archivage intermédiaire) à compter du départ du salarié.
- les données relatives aux cartes bancaires doivent être supprimées une fois la transaction réalisée.

(2) Données sensibles : révélant l'origine prétendument raciale ou ethnique ; portant sur les opinions politiques, philosophiques ou religieuses ; relatives à l'appartenance syndicale ; concernant la santé ou l'orientation sexuelle ; génétiques ou biométriques des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

3 - INFORMEZ LE DROIT DES PERSONNES

Permettez aux personnes d'exercer facilement leurs droits

Dès que vous collectez des données personnelles, le support utilisé doit comporter des mentions d'information :

• pourquoi vous collectez les données « la finalité » ; par exemple pour gérer les contrats d'entretien ;
• ce qui vous autorise à traiter ces données : il peut s'agir de l'exécution d'un contrat ;
• qui a accès aux données (ex : service facturation, paye)
• combien de temps vous les conservez (exemple : « 3 ans après la fin de la relation contractuelle ») ;
• les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via un message sur une adresse email dédiée, par un courrier postal) ;

Éviter des mentions trop longues. Vous pouvez par exemple, donner un premier niveau d'information en fin de formulaire/devis et renvoyer à une politique de confidentialité/vie privée sur vos conditions générales de ventes.

■ Mention d'information devis/facture

Le service _____(citer le nom du ou des services responsables du traitement) dispose de moyens informatiques destinés à gérer plus facilement _____ (indiquer la finalité du traitement). Conformément à la loi «Informatique et Libertés» du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à _____ (préciser le service et l'adresse). Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant.

■ Exemples de formulations pour obtenir l'accord de vos clients

Si vous ne souhaitez pas recevoir nos offres commerciales, merci de cocher cette case ☐
Si vous ne souhaitez pas recevoir des offres de nos partenaires, merci de cocher cette case ☐
Si vous ne souhaitez pas recevoir de notre part des offres commerciales pour nos produits ou services analogues à ceux que vous avez déjà achetés, merci de cocher cette case ☐

A noter : Si la case n'est pas cochée ? S'il n'a pas dit «non», c'est «oui».

4 - SÉCURISEZ VOS DONNÉES

■ Mesures simples et rapides

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.

Modèle de courrier à faire signer à vos salariés utilisateurs des données, disponible à la CAPEB 87.

LES 6 BONS RÉFLEXES

1 ■ **Ne collectez que les données vraiment nécessaires.** Posez-vous les bonnes questions.
Quel est mon objectif ? Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ? Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?

2 ■ **Soyez transparent**
Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes dont vous traitez les données.

3 ■ **Pensez aux droits des personnes**
Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.

4 ■ **Gardez la maîtrise de vos données**
Le partage et la circulation des données personnelles doivent être encadrées et contractualisées, afin de leur assurer une protection à tout moment.

5 ■ **Identifiez les risques**
Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer.

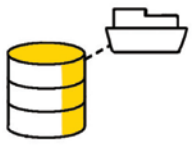
6 ■ **Sécurisez vos données**
Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

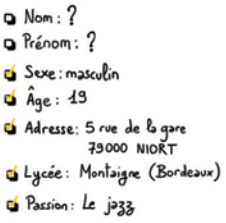
QU'EST-CE QU'UNE DONNÉE PERSONNELLE

Une personne peut être identifiée :

■ directement (exemple : nom, prénom) ;

■ indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).





L'identification d'une personne physique peut être réalisée :

• à partir d'une seule donnée (exemple : numéro de sécurité sociale) ;

• à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

POUR ALLER PLUS LOIN

■ **Votre entreprise utilise un site « vitrine »**, quelques réflexes de base sont à retenir.
- « mentions CNIL » en bas du formulaire de contact.
- un moyen de contact pour que les personnes puissent exercer leurs droits par voie électronique.
- mentions légales identifiant l'éditeur du site.

■ **Avis en ligne des consommateurs**

Les entreprises qui collectent, modèrent ou diffusent des avis en ligne des consommateurs, devront s'assurer des modalités de fonctionnement conformes à la réglementation.
Il doit être indiqué, de manière claire et visible, à proximité des avis :
- l'existence ou non d'une procédure de contrôle des avis ;
- la date de publication de chaque avis et leurs éventuelles mises à jour, la date de l'expérience de consommation concernée par l'avis ;
- les critères de classement des avis parmi lesquels figure le classement chronologique.

Il doit être tenu une rubrique spécifique facilement accessible dans laquelle seront mentionnés :
- l'existence ou non de contrepartie fournie en échange du dépôt d'avis ;
- le délai maximum de publication et de conservation d'un avis.

■ **Votre entreprise utilise Twitter, Facebook,** et autres réseaux sociaux, prévoyez :
- de rendre accessible un article ou un lien qui mène vers une page d'information sur les droits.
-d'anticiperleseffetsd'uneopérationdecommunication en ligne. Une réponse type aux internautes mécontents, qui exerceraient, par exemple leur droit d'opposition. La réactivité et l'efficacité de votre réponse contribuent à votre e-reputation.

POUR EN SAVOIR PLUS :
Connectez-vous sur le site internet de la CNIL ou
Appelez la CAPEB 87 au 05 55 77 92 00

Source : CNIL BPI France Le Lab Guide pratique de sensibilisation pour les petites et moyennes entreprises les grandes étapes pour protéger les données personnelles de votre entreprise au RGPD.

CAPEB L'Artisanat du Bâtiment HAUTE-VIENNE
24, Rue Lesage - BP 217 - 87006 LIMOGES
Tél : 05 55 77 92 00
secretariat@capeb87.fr