

RGPD : l'essentiel pour une TPE/PME

Registre, consentement, durées de conservation : la mise en conformité pragmatique, sans jargon.

15 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/rgpd-tpe-pme

Le RGPD s'applique à toute entreprise qui traite des données personnelles — clients, prospects, salariés — quelle que soit sa taille. Au-delà de l'obligation légale, une bonne hygiène des données est un argument de confiance vis-à-vis de vos clients, et de plus en plus une exigence de leurs appels d'offres. Ce guide déroule la mise en conformité pragmatique d'une TPE/PME : principes, bases légales, registre pas à pas, site web, sous-traitants, droits des personnes et gestion d'une violation.

1. Le RGPD en deux minutes

Une « donnée personnelle » est toute information se rapportant à une personne identifiable : nom, email (même professionnel : prenom.nom@entreprise.fr), téléphone, adresse IP, photo, données de paie... Un « traitement » est tout ce qu'on en fait : collecter, stocker, consulter, transmettre. Dès que votre entreprise a des clients, des prospects ou des salariés, elle traite des données personnelles et le RGPD s'applique — il n'y a pas de seuil de taille.

La logique du texte tient en une phrase : vous devez savoir quelles données vous détenez, pourquoi, pour combien de temps, les protéger correctement, et pouvoir le démontrer. Ce dernier point — la « responsabilité » (accountability) — explique l'importance de la documentation : en cas de contrôle, ce qui n'est pas documenté n'existe pas.

2. Les principes fondamentaux

- Finalité : on ne collecte des données que pour un usage précis, annoncé à la personne — pas « au cas où »
- Minimisation : uniquement les données nécessaires à cet usage (le formulaire de contact n'a pas besoin de la date de naissance)
- Exactitude : les données doivent être tenues à jour, et rectifiables
- Durée limitée : les données se suppriment ou s'archivent quand elles ne servent plus (ex. 3 ans après le dernier contact pour un prospect)
- Sécurité : protection proportionnée à la sensibilité (article 32 : chiffrement, contrôle des accès, sauvegardes...)
- Transparence et droits : les personnes savent ce que vous faites de leurs données et peuvent exercer leurs droits (accès, rectification, effacement, opposition, portabilité)

3. Les bases légales : le « pourquoi j'ai le droit »

Chaque traitement doit reposer sur une des six bases légales du règlement. Quatre concernent le quotidien d'une PME :

Le contrat

Gérer les données d'un client pour exécuter la prestation, facturer, livrer : pas besoin de consentement, c'est la base « exécution du contrat ».

L'obligation légale

Conserver les factures 10 ans, les données de paie, les déclarations sociales : la loi vous l'impose, c'est votre base légale.

L'intérêt légitime

La prospection B2B raisonnable (contacter un professionnel sur son adresse pro pour un sujet en rapport avec sa fonction), la sécurité de vos systèmes, la défense en justice. L'intérêt légitime exige un équilibre : la personne doit pouvoir s'y opposer facilement.

Le consentement

Nécessaire pour la prospection par email vers les particuliers (B2C), les cookies non essentiels, les newsletters. Un consentement valide est libre, spécifique, éclairé et révocable — la case pré-cochée ne compte pas.

CAS CONCRET

Un artisan a le droit d'envoyer un devis puis des rappels à son client (contrat), de garder la facture 10 ans (obligation légale), de recontacter un prospect professionnel rencontré sur un salon (intérêt légitime) — mais pas d'inscrire d'office à sa newsletter tous les emails collectés, sans case à cocher (consentement requis).

4. Le registre des traitements, pas à pas

Le registre est LE document de base — obligatoire dans la quasi-totalité des cas, et premier document demandé en cas de contrôle. La CNIL fournit un modèle simplifié pour les PME ; comptez une demi-journée pour une petite structure. Pour chaque traitement, notez :

- Le nom et la finalité : « gestion des clients et facturation », « recrutement », « prospection », « paie », « vidéosurveillance »...
- Les catégories de données : identité, coordonnées, données bancaires, données RH...
- Les personnes concernées et qui accède aux données en interne
- Les destinataires externes : expert-comptable, logiciel de paie, hébergeur, CRM...
- Les durées de conservation, en distinguant base active et archivage
- Les mesures de sécurité appliquées

BON À SAVOIR

Une TPE type a rarement plus de 6 à 8 traitements : clients/facturation, prospects, fournisseurs, paie et RH, recrutement, site web/contact, newsletter, éventuellement vidéosurveillance. Commencez par les lister — le reste du registre en découle.

5. Le site web : la partie visible de votre conformité

- Une politique de confidentialité claire et à jour : quelles données, pourquoi, combien de temps, quels droits et comment les exercer
- Les cookies non essentiels (mesure d'audience, publicité) déposés uniquement après consentement — le bandeau doit permettre de refuser aussi simplement que d'accepter

- Les formulaires ne collectent que le nécessaire et renvoient vers la politique de confidentialité
- Newsletter : inscription par action volontaire, désinscription en un clic dans chaque envoi
- Le site en HTTPS — une page de contact en HTTP est déjà un manquement à l'article 32

6. Sous-traitants : l'article 28

Tout prestataire qui traite des données pour votre compte — hébergeur, éditeur SaaS, agence web, expert-comptable, service d'emailing — est un « sous-traitant » au sens du RGPD. Vous restez responsable des données que vous lui confiez.

- Un contrat ou des CGV incluant les clauses de l'article 28 (les grands acteurs les intègrent dans leur « Data Processing Agreement » — vérifiez qu'il existe)
- La localisation des données : un hébergement UE simplifie tout ; hors UE, il faut un mécanisme de transfert valide
- Une liste tenue à jour de vos sous-traitants, dans le registre
- En sens inverse : si VOS clients vous confient des données, c'est vous le sous-traitant — attendez-vous à devoir signer ces mêmes clauses

7. Répondre à une demande de droit

Toute personne peut demander l'accès à ses données, leur rectification, leur effacement ou s'opposer à leur usage. Vous avez un mois pour répondre — gratuitement.

- Désigner en interne qui reçoit et traite ces demandes
- Vérifier l'identité du demandeur en cas de doute, sans exiger plus que nécessaire
- Répondre même quand la réponse est négative, en expliquant pourquoi (ex. : obligation légale de conserver la facturation malgré une demande d'effacement)
- Garder une trace de la demande et de la réponse — c'est la démonstration de conformité

8. Violation de données : les 72 heures

Une « violation » est tout incident touchant des données personnelles : piratage, ransomware, envoi au mauvais destinataire, vol d'un portable non chiffré, perte de sauvegardes.

- Documenter TOUTE violation dans un registre interne, même mineure et non notifiée
- Notifier la CNIL sous 72 h si la violation présente un risque pour les personnes (le formulaire est en ligne sur cnil.fr)
- Informer directement les personnes concernées si le risque est élevé (données bancaires, mots de passe, données sensibles)
- Le compte à rebours des 72 h démarre à la découverte de la violation — d'où l'intérêt d'avoir préparé la procédure avant

ATTENTION

Ne pas notifier en espérant que ça passe est le pire calcul : la violation finit souvent par se savoir (données publiées, plainte d'un client), et l'absence de notification devient alors une infraction distincte, lourdement sanctionnée. Une notification honnête et documentée est au contraire perçue comme une preuve de sérieux.

9. Contrôles et sanctions : ce qui arrive vraiment aux PME

Les amendes records des géants du numérique font les titres, mais la CNIL contrôle et sanctionne aussi les PME — le plus souvent après une plainte (client mécontent, salarié en litige) ou une violation médiatisée. Les sanctions vont du rappel à l'ordre à l'amende (jusqu'à 4 % du chiffre d'affaires mondial en théorie ; en pratique, des amendes de quelques milliers à quelques dizaines de milliers d'euros pour les PME, via une procédure simplifiée).

Les manquements les plus sanctionnés chez les petites structures : prospection sans consentement, vidéosurveillance excessive des salariés, absence de registre, sécurité négligée, et non-coopération avec la CNIL. Autant de points qui se corrigent avec le socle décrit dans ce guide.

L'essentiel à retenir

- 01 Créer le registre des traitements (modèle CNIL) et le tenir à jour
- 02 Identifier la base légale de chaque traitement
- 03 Publier une politique de confidentialité à jour sur le site
- 04 Mettre le bandeau cookies en conformité (refus aussi simple que l'accord)
- 05 Vérifier les contrats article 28 de tous vos sous-traitants
- 06 Définir des durées de conservation et purger régulièrement
- 07 Désigner qui répond aux demandes de droits (délai : un mois)
- 08 Préparer la procédure de notification CNIL sous 72 h

Questions fréquentes

Dois-je désigner un DPO (délégué à la protection des données) ?

C'est obligatoire seulement si votre cœur d'activité implique un suivi régulier et systématique de personnes à grande échelle, ou des données sensibles à grande échelle — rarement le cas d'une TPE/PME classique. En revanche, désigner un référent interne (même non officiel) qui porte le sujet est une bonne pratique, et un DPO externalisé mutualisé est une option abordable si vos traitements sont sensibles.

Les adresses email professionnelles sont-elles des données personnelles ?

Oui dès qu'elles identifient une personne : prenom.nom@entreprise.fr est une donnée personnelle, contact@entreprise.fr ne l'est pas. La prospection B2B vers une adresse nominative reste possible sur la base de l'intérêt légitime, à condition que le message soit en rapport avec la fonction du destinataire et qu'il puisse s'opposer simplement.

Combien de temps conserver les données de mes clients et prospects ?

Repères usuels : prospects, 3 ans après le dernier contact ; données clients actives, la durée de la relation commerciale ; factures et pièces comptables, 10 ans (obligation légale) ; bulletins de paie, 5 ans côté employeur ; candidatures non retenues, 2 ans maximum sauf accord. L'important est de fixer VOS durées dans le registre et de les appliquer.

Google Analytics, Microsoft 365, un CRM américain : ai-je le droit ?

La question des transferts hors UE évolue régulièrement (accords successifs entre l'UE et les États-Unis). En pratique : privilégiez les options d'hébergement UE quand elles existent, vérifiez que le prestataire propose un DPA et des clauses de transfert valides, et pour la mesure d'audience, les alternatives européennes ou les configurations exemptées de consentement simplifient beaucoup la conformité.

Par quoi commencer si nous n'avons jamais rien fait ?

Dans l'ordre : 1) le registre des traitements — il révèle tout le reste ; 2) le site web (politique de confidentialité, cookies, HTTPS) — c'est la partie visible ; 3) les durées de conservation et une première purge ; 4) les contrats sous-traitants ; 5) la procédure violation/droits. Une TPE motivée fait l'essentiel en quelques jours étalés sur un mois.

Pour aller plus loin

CNIL — Guide de la sécurité des données personnelles — www.cnil.fr/fr/un-guide-de-la-securite-des-donnees-personnelles

CNIL — Modèle de registre simplifié — www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

CNIL — Notifier une violation de données — www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Bpifrance — Guide RGPD TPE/PME (avec la CNIL) — www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr