DOCUMENT 03

Registre des activités de traitement RGPD

Modèle conforme à l'article 30 du RGPD pour les PME : traitements, sous-traitants, violations de données et exercice des droits.

Entreprise		Date		Version	

Mode d'emploi

- **Qui doit le tenir ?** Toute entreprise qui traite des données personnelles de façon non occasionnelle (clients, salariés, prospects, fournisseurs…) : en pratique, la quasi-totalité des PME, malgré l'allègement prévu sous 250 salariés.
- **Un traitement = une finalité.** Listez ce que vous faites avec des données personnelles (paie, gestion clients, recrutement, vidéosurveillance, site web…), pas chaque fichier.
- **Le registre doit être à jour et consultable** à la demande de la CNIL. Il se révise à chaque nouvelle activité, nouvel outil ou nouveau sous-traitant.
- **Cinq lignes d'exemple** sont pré-remplies en gris : adaptez-les à votre réalité.

A. Identité du responsable de traitement

Raison sociale / SIREN	
Adresse	
Représentant légal	
Référent RGPD ou DPO (nom, contact)	
Date de création / dernière mise à jour	

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

B. Registre des traitements

N°	Traitement et finalité	Personnes concernées	Catégories de données	Destinataires	Base légale	Durée de conservation	Hors UE ?	Mesures de sécurité
1	***Gestion de la paie et du personnel*** *— établir les salaires, respecter les obligations sociales*	*Salariés*	*Identité, coordonnées, n° SS, RIB, situation familiale, données de paie*	*Service RH, expert-comptable, organismes sociaux*	*Obligation légale / contrat*	*Bulletins : 5 ans (copie employeur) ; dossier personnel : durée du contrat + délais légaux*	*Non*	*Accès restreint RH, authentification multifacteur, sauvegardes chiffrées*
2	***Gestion de la clientèle*** *— contrats, facturation, suivi commercial*	*Clients, contacts*	*Identité, coordonnées, historique commercial, factures*	*Commercial, comptabilité, prestataire CRM*	*Contrat*	*Durée de la relation + 5 ans ; pièces comptables : 10 ans*	*[ ]*	*Comptes nominatifs, droits par profil, journalisation*
3	***Prospection commerciale***	*Prospects*	*Identité, coordonnées professionnelles, centres d'intérêt*	*Commercial, outil d'e-mailing*	*Intérêt légitime (B2B) / consentement (B2C)*	*3 ans après le dernier contact*	*[ ]*	*Lien de désinscription, accès restreint*
4	***Recrutement***	*Candidats*	*CV, lettre, coordonnées, parcours*	*RH, managers concernés*	*Mesures précontractuelles*	*2 ans max. après le dernier contact (sauf accord pour conserver)*	*Non*	*Stockage sécurisé, accès limité aux recruteurs*
5	***Sécurité informatique et journalisation***	*Salariés, prestataires*	*Identifiants, journaux de connexion, adresses IP*	*Référent IT, prestataire*	*Intérêt légitime (sécurité)*	*6 mois à 1 an*	*[ ]*	*Accès administrateurs restreint, journaux protégés*

Vos traitements — complétez ci-dessous (ajoutez des lignes en dupliquant la page si nécessaire).

N°	Traitement et finalité	Personnes concernées	Catégories de données	Destinataires	Base légale	Durée de conservation	Hors UE ?	Mesures de sécurité
6								
7								
8								
9								

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

N°	Traitement et finalité	Personnes concernées	Catégories de données	Destinataires	Base légale	Durée de conservation	Hors UE ?	Mesures de sécurité
10								
11								

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

C. Registre des sous-traitants (art. 28)

Tout prestataire qui traite des données personnelles pour votre compte (hébergeur, logiciel en ligne, expert-comptable, prestataire informatique, paie externalisée, e-mailing…) doit être lié à vous par un **contrat de sous-traitance** (DPA).

Sous-traitant	Service rendu / données traitées	Pays d'hébergement	Contrat art. 28 signé	Date	Garanties hors UE	Contact DPO / sécurité

D. Registre des violations de données (art. 33-34)

Toute violation (perte, vol, accès non autorisé, envoi erroné, rançongiciel…) est consignée, même si elle n'est pas notifiée. Si elle est susceptible d'engendrer un risque pour les personnes, la **notification à la CNIL est obligatoire dans les 72 heures** après en avoir pris connaissance ; si le risque est élevé, les personnes concernées sont également informées.

Date de découverte	Nature de la violation	Données et personnes concernées	Nb personnes	Notifiée CNIL (date)	Personnes informées	Mesures prises / enseignements

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

E. Procédure d'exercice des droits des personnes

Les personnes concernées (clients, salariés, candidats) peuvent demander l'accès à leurs données, leur rectification, leur effacement, la limitation ou l'opposition, et la portabilité. **Réponse sous un mois** (prolongeable de deux mois si la demande est complexe, avec information de la personne).

Étape	Action	Responsable
1. Réception	Enregistrer la demande (date, demandeur, nature) et accuser réception. Toute personne de l'entreprise qui reçoit une demande la transmet au référent RGPD le jour même.	Tous / référent
2. Vérification d'identité	S'assurer de l'identité du demandeur, avec une demande de justificatif seulement si un doute existe.	Référent RGPD
3. Recherche	Identifier les données concernées dans tous les systèmes (y compris messagerie, sauvegardes, sous-traitants).	Référent / IT
4. Réponse	Répondre par écrit, de façon claire, dans le délai d'un mois. En cas de refus, motiver et indiquer la possibilité de saisir la CNIL.	Direction / référent
5. Traçabilité	Consigner la demande et la réponse dans le registre des demandes.	Référent RGPD

F. Registre des demandes d'exercice de droits

Date de réception	Demandeur	Droit exercé	Date de réponse	Délai respecté ?	Suite donnée

Points d'attention de l'expert

• Mentions d'information (RGPD art. 13/14) sur votre site, vos formulaires, vos contrats de travail et vos affichages de vidéosurveillance. • Données sensibles (santé, syndicats…) : traitement exceptionnel, sécurité renforcée. • Cookies et traceurs : consentement préalable pour les traceurs non essentiels. • Une analyse d'impact (AIPD) est requise pour les traitements à risque élevé (surveillance systématique, données sensibles à grande échelle).

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.