

MODÈLE

Registre des traitements RGPD (article 30) : le modèle prêt à remplir pour PME

Colonnes obligatoires, lignes types (paie, clients, prospection, vidéosurveillance) et cadre d'usage — sans jargon.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~11 min Édition 2026 sedona-ai.com

Le registre des activités de traitement est votre inventaire vivant de tous les usages de données personnelles dans l'entreprise. L'article 30 du RGPD le rend obligatoire pour tout responsable de traitement, et la dérogation « moins de 250 salariés » ne vous protège quasiment jamais dès que vous faites de la paie ou de la vidéosurveillance. Ce modèle reprend les colonnes exigées, propose quatre lignes types à adapter, et vous dit exactement quoi inscrire entre chaque [crochet].

À retenir

- Le registre (art. 30) est obligatoire pour tout responsable de traitement et doit être présenté à la CNIL sur simple demande.
- La dérogation « moins de 250 salariés » est quasi inopérante : paie récurrente, vidéosurveillance ou données sensibles la font sauter.
- Sept champs minimum : responsable, finalités, personnes et données concernées, destinataires, transferts hors UE, durées de conservation, mesures de sécurité.
- Quatre lignes types couvrent l'essentiel d'une PME : paie/RH, clients/facturation, prospection commerciale, vidéosurveillance.
- Le registre n'est pas une AIPD : il recense tout, l'analyse d'impact ne concerne que les traitements à risque élevé.
- Le format est libre (tableur suffit) ; ce qui compte, c'est un registre tenu à jour à chaque nouveau traitement.

01 Comment utiliser ce modèle

Ce document est un cadre à remplir, pas une lecture théorique. Créez un tableur (une ligne = un traitement), reprenez les colonnes de la section « Les colonnes de votre registre », puis adaptez les quatre lignes types fournies plus bas à votre réalité. Partout où vous voyez du texte [entre crochets], remplacez-le par vos propres informations.

1. Recensez vos traitements

Faites le tour des services (RH, commerce, compta, sécurité). Chaque usage récurrent de données personnelles = une ligne : [ex. gestion de la paie], [gestion clients], [prospection], [vidéosurveillance].

2. Remplissez une ligne par traitement

Pour chacun, renseignez les 6 à 8 champs de l'article 30 (voir plus bas). En cas de doute sur une case, inscrivez [à préciser] plutôt que de laisser vide.

3. Désignez un pilote et une date de revue

Notez en tête du registre : [nom du responsable du registre] et [date de dernière mise à jour]. Fixez une revue au moins annuelle.

4. Mettez à jour à chaque changement

Nouveau logiciel, nouveau prestataire, nouveau transfert hors UE, nouvelle finalité : le registre se met à jour immédiatement, pas une fois par an seulement.

Un point de départ officiel et gratuit

La CNIL met à disposition un modèle de registre simplifié au format tableur (ODS), pensé pour les PME, TPE, associations et petites collectivités. Vous pouvez partir de ce fichier officiel et l'enrichir avec les lignes types de ce document.

02 Ce qu'impose vraiment l'article 30

Le registre des activités de traitement est l'outil central du principe de responsabilité (accountability) : il prouve que vous savez quelles données vous traitez, pourquoi et comment. Pour un responsable de traitement, l'article 30.1 fixe un contenu minimal — ni plus, ni moins.

- Nom et coordonnées du responsable de traitement (et, le cas échéant, du représentant, du co-responsable et du DPO)
- Finalités du traitement (à quoi servent les données)
- Catégories de personnes concernées et catégories de données traitées
- Catégories de destinataires des données
- Transferts vers un pays tiers ou une organisation internationale, avec la documentation des garanties le cas échéant
- Durées de conservation prévues pour chaque catégorie de données
- Description générale des mesures de sécurité techniques et organisationnelles

Forme libre, mise à disposition obligatoire

Le registre peut être tenu sur papier ou sous forme électronique — un tableur suffit. L'obligation ne porte pas sur un format technique imposé, mais sur le contenu et sur la capacité à présenter le registre à l'autorité de contrôle sur demande.

03 « Moins de 250 salariés = pas de registre » : le contresens à éviter

C'est l'erreur la plus fréquente. La dérogation de l'article 30(5) existe bien pour les organismes de moins de 250 salariés, mais elle tombe dès que l'une de ces trois conditions est remplie : le traitement présente un risque pour les droits et libertés des personnes, il n'est pas occasionnel, ou il porte sur des données sensibles (santé, biométrie...) ou relatives aux condamnations et infractions.

En pratique, la dérogation ne vous protège presque jamais

Dès qu'il y a de la paie (traitement RH récurrent, donc non occasionnel), de la vidéosurveillance (souvent jugée à risque pour les personnes) ou des données de santé, l'exception saute et le registre complet redevient obligatoire. La CNIL recommande d'ailleurs, en cas de doute, d'intégrer quand même le traitement au registre.

250

Seuil de salariés de la dérogation art. 30(5) — mais quasi inopérant dès qu'il y a paie, vidéosurveillance ou données sensibles

CNIL — Le registre des activités de traitement, 2020

04 Les colonnes de votre registre

Reprenez ces colonnes telles quelles dans votre tableur. Elles couvrent l'intégralité du contenu minimal de l'article 30.1 ; ajoutez une colonne « base légale » (article 6 du RGPD), très utile pour piloter et justifier chaque traitement.

Colonne	À y inscrire
Nom du traitement	[Intitulé clair, ex. Gestion de la paie]
Finalité(s)	[Pourquoi ce traitement existe]
Base légale (art. 6)	[Consentement / contrat / obligation légale / intérêt légitime...]
Personnes concernées	[Salariés, clients, prospects, visiteurs...]
Catégories de données	[Identité, coordonnées, données bancaires, images...]
Destinataires	[Services internes, prestataires, organismes sociaux...]
Transfert hors UE	[Non / Oui + pays + garanties]
Durée de conservation	[Durée par catégorie de données]
Mesures de sécurité	[Contrôle d'accès, chiffrement, sauvegardes...]

Les 6 bases légales possibles

L'article 6 du RGPD ne reconnaît que six fondements : consentement, exécution d'un contrat, obligation légale, sauvegarde des intérêts vitaux, mission d'intérêt public, intérêt légitime. Chaque ligne de votre registre doit pouvoir se rattacher à l'une d'elles.

05 Quatre lignes types à adapter (PME)

Voici quatre traitements que l'on retrouve dans presque toutes les PME. Recopiez-les, puis ajustez chaque case à votre situation. Les durées de conservation ci-dessous sont volontairement laissées à préciser : elles dépendent de textes dédiés (code du travail, doctrine CNIL vidéoprotection...) qu'il faut vérifier avant d'inscrire un chiffre.

Traitement	Finalité	Base légale	Personnes / Données	Destinataires	Conservation
Paie / gestion RH	Verser les salaires, remplir les obligations sociales	Exécution du contrat de travail + obligation légale	Salariés / identité, RIB, cotisations	Expert-comptable, organismes sociaux	[Durées légales du code du travail — à préciser]
Gestion clients / facturation	Gérer la relation commerciale et facturer	Exécution du contrat	Clients / identité, coordonnées, données de facturation	Compta, prestataire de paiement	[Durée de la relation + prescriptions légales]
Prospection commerciale	Contacter des prospects, envoyer des offres	Consentement (B2C) ou intérêt légitime (B2B)	Prospects / identité, coordonnées pro	Équipe commerciale, outil d'emailing	[Durée limitée après dernier contact — à préciser]
Vidéosurveillance	Sécurité des biens et des personnes	Intérêt légitime	Salariés, visiteurs / images	Responsable sécurité, forces de l'ordre sur réquisition	[Durée courte — à valider via la fiche CNIL vidéoprotection]

N'inventez pas de durées de conservation

Les durées exactes (bulletins de paie, images de vidéosurveillance...) sont encadrées par des textes précis. Laissez [à préciser] et vérifiez chaque durée à sa source — code du travail, fiches CNIL — avant de figer un chiffre dans votre registre.

06 Registre responsable ≠ registre sous-traitant

Attention à ne pas mélanger deux obligations distinctes. Ce modèle est le registre du responsable de traitement (art. 30.1) : c'est celui qui concerne la paie, les clients, la prospection et la vidéosurveillance de votre entreprise.

Si votre entreprise traite aussi des données pour le compte de clients (vous êtes alors sous-traitant), l'article 30.2 impose un second registre, au contenu différent : identité des clients responsables, sous-traitants ultérieurs, catégories de traitements réalisés pour autrui, transferts et mesures de

07 Le registre n'est pas une AIPD — et il doit rester vivant

Le registre recense tous vos traitements ; l'analyse d'impact (AIPD, art. 35) est une analyse de risque approfondie, requise uniquement pour les traitements à risque élevé. Les deux sont complémentaires : c'est en tenant votre registre que vous repérez quels traitements méritent une AIPD.

Un registre vivant, pas une case à cocher

Le registre est un outil de pilotage de la conformité, au titre du principe de responsabilité (art. 5.2). Mettez-le à jour à chaque nouveau traitement, nouvelle finalité, nouveau prestataire ou nouveau transfert hors UE — pas seulement lors d'un contrôle.

56

Fiches de traitement dans le registre RGPD que la CNIL publie à titre d'exemple pédagogique (pour illustrer, pas à recopier)

CNIL — Le registre RGPD de la CNIL, mai 2026

08 Où Sedona peut vous aider

Le registre décrit ici est une brique de conformité RGPD. L'article 32 du RGPD demande de tester, d'analyser et d'évaluer régulièrement l'efficacité des mesures de sécurité : Sedona Radar analyse ce que votre domaine expose sur Internet et remet un rapport daté, que vous pouvez verser à votre dossier de conformité. Pour ses propres services, Sedona fournit sur demande un accord de sous-traitance (DPA) et liste ses sous-traitants ; les données sont stockées dans l'Union européenne.

Ce que Sedona fait — et ne fait pas

Sedona Radar donne des indicateurs de maturité sur plusieurs référentiels (dont NIS2 et Hygiène ANSSI) mais ne certifie rien. Sedona.AI n'est ni qualifiée PASSI ni certifiée ISO 27001, et n'établit pas votre registre RGPD à votre place.

§ Sources

1. CNIL — Le registre des activités de traitement (contenu obligatoire, dérogation art. 30(5), modèle) — <https://www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement>
2. CNIL — Modèle de registre simplifié (fichier ODS téléchargeable) — <https://www.cnil.fr/sites/cnil/files/atoms/files/registre-traitemment-simplifie.ods>
3. CNIL — La CNIL publie un nouveau modèle de registre simplifié — <https://www.cnil.fr/fr/la-cnil-publie-un-nouveau-modele-de-registre-simplifie>
4. CNIL — Le registre RGPD de la CNIL (exemple pédagogique, 56 fiches) — <https://www.cnil.fr/fr/le-registre-rgpd-de-la-cnil>
5. CNIL — Registre des activités de traitement (définition) — <https://www.cnil.fr/fr/definition/registre-des-activites-de-traitement>

6. CNIL — Cartographier vos traitements de données personnelles — <https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles>
7. Texte de l'article 30 RGPD — Registre des activités de traitement — <https://www.privacy-regulation.eu/fr/30.htm>
8. Texte de l'article 6 RGPD — Licéité du traitement (bases légales) — <https://www.privacy-regulation.eu/fr/6.htm>

Article 32 du RGPD : testez régulièrement ce que vous exposez

Le RGPD demande de tester régulièrement l'efficacité de vos mesures de sécurité. Sedona Radar analyse ce que votre domaine expose sur Internet et remet un rapport en français, avec un plan de correction. Lancez un scan gratuit.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit