

Le registre des activités de traitement

Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que vous faites avec les données personnelles.

Le registre est prévu par [l'article 30 du RGPD](#). Il participe à la documentation de la conformité.

Document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles et vous permet d'identifier précisément :

- **les parties prenantes** (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
- **les catégories de données traitées**,
- **à quoi servent ces données** (ce que vous en faites), **qui accède** aux données et **à qui elles sont communiquées**,
- **combien de temps vous les conservez**,
- **comment elles sont sécurisées**.

Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est un outil de pilotage et de démonstration de votre conformité au RGPD. Il vous permet de documenter vos traitements de données et de vous poser les bonnes questions : ai-je vraiment besoin de cette donnée dans le cadre de mon traitement ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc.

Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle vous permettra d'en déduire un plan d'action de mise en conformité de vos traitements aux règles de protection des données.

La CNIL présente ici les éléments essentiels relatifs au registre et propose également un modèle de base répondant aux conditions posées par le RGPD.

Qui est concerné ?

L'obligation de tenir un registre des traitements **concerne tous les organismes, publics comme privés et quelle que soit leur taille**, dès lors qu'ils [traitent des données personnelles](#).

Dispositions pour les organismes de moins de 250 salariés

Les entreprises de moins de 250 salariés bénéficient d'une dérogation en ce qui concerne la tenue de registres. **Ils doivent inscrire au registre les seuls traitements de données suivants :**

- les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ;
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.)
- les traitements qui portent sur des données sensibles (exemple : données de santé, infractions, etc.).

En pratique, cette dérogation est donc limitée à des cas très particuliers de traitements, mis en œuvre de manière occasionnelle et non routinière, comme par exemple une campagne de communication à l'occasion de l'ouverture d'un nouvel établissement, sous réserve que ces traitements ne soulèvent aucun risque pour les personnes concernées. En cas de doute sur l'application de cette dérogation à un traitement, la CNIL vous recommande de l'intégrer dans votre registre.

Un registre spécifique pour les activités de sous-traitance des données personnelles

Les organismes qui traitent des données personnelles **pour le compte d'un autre organisme** (les sous-traitants comme, par exemple, des prestataires de services informatiques ou des agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients) doivent également tenir un registre de leurs activités de sous-traitant impliquant le traitement de données.

Pour plus de précisions : [voir le guide RGPD pour les sous-traitants](#)

Que contient le registre ?

L'article 30 du RGPD prévoit des obligations spécifiques pour le registre du responsable de traitement de données personnelles et pour le registre du sous-traitant. Si votre organisme agit à la fois en tant que sous-traitant et responsable de traitement, votre registre doit donc clairement distinguer les deux catégories d'activités.

En pratique, dans cette hypothèse, la CNIL vous recommande de tenir 2 registres :

1. un pour les traitements de données personnelles dont vous êtes vous-même responsable,
2. un autre pour les traitements que vous opérez, en tant que sous-traitant, pour le compte de vos clients.

- [1. Le registre du responsable de traitement](#)
- [2. Le registre du sous-traitant](#)

Le registre du responsable de traitement **doit recenser l'ensemble des traitements mis en œuvre par votre organisme.**

En pratique, une fiche de registre doit donc être établie pour chacune de ces activités.

Ce registre doit comporter **le nom et les coordonnées de votre organisme** ainsi que, le cas échéant, [de votre représentant, si votre organisme n'est pas établi dans l'Union européenne](#), et de votre [délégué à la protection des données](#) si vous en disposez.

En outre, **pour chaque activité de traitement**, la fiche de registre doit comporter au moins les éléments suivants :

1. le cas échéant, **le nom et les coordonnées** du [responsable conjoint du traitement](#) mis en œuvre
2. les **finalités** du traitement, l'objectif en vue duquel vous avez collecté ces données

3. les catégories de **personnes concernées** (client, prospect, employé, etc.)
4. les catégories de **données personnelles** (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, données de localisation, etc.)
5. les **catégories de destinataires** auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants auxquels vous recourez
6. les **transferts** de données à caractère personnel vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces transferts ;
7. les **délais prévus pour l'effacement** des différentes catégories de données, c'est-à-dire la durée de conservation, ou à défaut les critères permettant de la déterminer
8. dans la mesure du possible, une **description générale des mesures de sécurité** techniques et organisationnelles que vous mettez en œuvre

Le registre du sous-traitant **doit recenser toutes les catégories d'activités de traitement effectuées pour le compte de vos clients.**

En pratique, une fiche de registre doit donc être établie pour chacune de ces catégories d'activités (hébergement de données, maintenance informatique, service d'envoi de messages de prospection commerciale, etc.).

Ce registre doit comporter **le nom et les coordonnées de votre organisme** ainsi que, le cas échéant, [de votre représentant, si votre organisme n'est pas établi dans l'Union européenne](#), et de votre [délégué à la protection des données](#) si vous en disposez.

Pour chaque catégorie d'activité effectuée pour le compte de clients, il doit contenir les éléments minimaux suivants :

1. le nom et les coordonnées de **chaque client, responsable de traitement**, pour le compte duquel vous traitez les données et, le cas échéant, le nom et les coordonnées de leur représentant
2. le **nom et les coordonnées des sous-traitants auxquels vous-même faites appel** dans le cadre de cette activité
3. les **catégories de traitements** effectués pour le compte de chacun de vos clients, c'est-à-dire les opérations effectivement réalisées pour leur compte (par exemple : pour la catégorie « service d'envoi de messages de prospection », il peut s'agir de la collecte des adresses mails, de l'envoi sécurisé des messages, de la gestion des désabonnements, etc.)
4. les **transferts de données** à caractère personnel vers un pays tiers ou à une organisation internationale. Dans les cas très particuliers mentionnés au 2^{ème} alinéa de l'article 49.1 (absence de décision d'adéquation en vertu de l'article 45 du RGPD, absence des garanties appropriées prévues à l'article 46 du RGPD et inapplicabilité des exceptions prévues au 1^{er} alinéa de l'article 49.1), les garanties prévues pour encadrer les transferts doivent être mentionnées.
5. dans la mesure du possible, une **description générale des mesures de sécurité** techniques et organisationnelles que vous mettez en œuvre.

Quelle forme doit prendre le registre ?

Le RGPD impose uniquement que **le registre se présente sous une forme écrite**. Le format du registre est libre et peut être constitué au format papier ou électronique.

Document reference

Modèles de registre

Pour faciliter la tenue de ce registre, la CNIL propose un modèle de registre de base (format PDF et Word), destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures (TPE-PME, associations, petites collectivités, etc.).

Ils permettent de satisfaire au socle d'exigences posées par l'article 30 du RGPD.

La CNIL recommande, dans la mesure du possible, d'enrichir le registre de mentions complémentaires afin d'en faire un outil plus global de pilotage de la conformité.

[RGPD - Modèle de registre \(pdf\)](#)

[PDF-369.31 Ko]

[RGPD - Modèle de registre \(Rtf\)](#)

[RTF-2.35 Mo]

Qui doit tenir le registre ?

Le registre doit être tenu par les responsables de traitement ou les sous-traitants eux-mêmes. Ils peuvent ainsi disposer d'une vue d'ensemble de toutes les activités de traitement de données à caractère personnel qu'ils effectuent.


Une personne au sein de l'organisme peut être spécifiquement chargée de la tenue du registre. Dans le cas où l'organisme a désigné un délégué à la protection des données (DPD), interne ou externe, celui-ci peut être chargé de la tenue du registre. Le registre pourra ainsi constituer l'un des outils permettant au délégué à la protection des données (DPO) d'exercer ses missions de contrôle du respect du RGPD ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant.

Comment constituer un registre ?

Recenser

Rassembler les informations disponibles 

Lister

Elaborer la liste des traitements 

Analyser

Affiner / préciser 

Comment constituer un registre ?

Recenser


Lister

Analyser

☐☐☐

line

Rassembler les informations disponibles 

Elaborer la liste des traitements 

Affiner / préciser 

- 1.
- 2.
- 3.

Rassembler les informations disponibles

- Identifier et rencontrer les responsables opérationnels des différents services susceptibles de traiter des données personnelles.
- Si l'organisme dispose d'un site internet, l'analyser et identifier les données collectées dans les formulaires en ligne (questionnaire, formulaire de contact, création d'un compte, etc.), les mentions d'information « protection des données », l'utilisation de cookies, etc.
- Pour vous aider, s'appuyer sur [la liste des traitements déclarés](#) à la CNIL.

Elaborer la liste des traitements

- Lister dans un tableau de suivi les différentes activités de l'organisme nécessitant le traitement de données personnelles. Les traitements de données doivent être identifiés par finalité et non par logiciel utilisé, car un même logiciel peut être utilisé pour différents traitements et inversement.
- Sur la base des informations collectées lors des entretiens, remplir une fiche de registre par activité.

Affiner / préciser

Sur la base de ce registre, identifier et analyser les risques qui peuvent peser sur les traitements de données mis en œuvre et élaborer un plan d'action de mise en conformité au RGPD.

A quelle fréquence faut-il mettre à jour le registre ?

Le registre doit être mise à jour régulièrement au gré des évolutions fonctionnelles et techniques des traitements de données. En pratique, toute modification apportée aux conditions de mise en œuvre de chaque traitement inscrit au registre (nouvelle donnée collectée, allongement de la durée de conservation, nouveau destinataire du traitement, etc.) doit être portée au registre.

A qui communiquer le registre ?

Par nature, le registre est un document interne et évolutif, qui doit avant tout aider l'organisme à piloter sa conformité.

Le registre doit toutefois pouvoir être communiqué à la CNIL lorsqu'elle le demande. Elle pourra en particulier l'utiliser dans le cadre de sa mission de contrôle des traitements de données.

- **Les organismes du secteur public** sont tenus de communiquer le registre à toute personne qui en fait la demande, car il s'agit d'un document administratif, communicable à tous, au sens du code des relations entre le public et l'administration. Toutefois, le registre communiqué doit être occulté de toute information dont la divulgation pourrait en particulier [porter atteinte aux secrets protégés par la loi, et notamment à la sécurité des systèmes d'information](#).
- **Les organismes privés** (non chargés d'une mission de service public) ne sont pas tenus de communiquer le registre au public. Néanmoins, ils peuvent, s'ils l'estiment opportun, le communiquer aux personnes qui en font la demande.

Bonnes pratiques

En enrichissant le registre avec des informations complémentaires, vous pouvez faire du registre un véritable outil de pilotage de votre conformité au RGPD. En effet, les obligations de documentation prévues par le RGPD ne se limitent pas à l'obligation de tenir un registre, prévue à l'article 30 du RGPD. Disposer, dans un même document, de toutes les informations relatives aux traitements que vous mettez en œuvre et exigées par le RGPD vous permettra de vous assurer, à chaque instant, de votre conformité aux règles de protection des données ou d'identifier les actions que vous devez mener pour atteindre cet objectif.

Ce registre **pourra également être utilisé par votre délégué à la protection des données pour accomplir l'ensemble de ses missions**, voire être consulté par tout collaborateur de l'organisme ayant vocation à mettre en œuvre des traitements de données.

- Par exemple, **en ajoutant à votre registre les informations nécessaires pour informer les personnes** (base légale du traitement, et selon le cas, fondement juridique du transfert de données vers des pays tiers, droits qui s'appliquent au traitement, existence ou non d'une décision automatisée, origine des données, etc.) vous pourrez vous appuyer sur votre registre pour rédiger vos mentions d'information.
- Vous pouvez également **consigner dans le registre un historique des violations de données et recenser tous les documents liés aux transferts** de données hors de l'Union européenne (clauses contractuelles, BCR, etc.) et aux sous-traitants auxquels vous recourez (contrats de sous-traitance)