cpme 71
SAÔNE-ET-LOIRE

Protégez-les

SOMMAIRE

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 donnée 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.

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.

Dispositif 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 registre. 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 : système de géolocalisation, de vidéosurveillance, etc., …)
- les traitements qui portent sur des données sensibles (exemple : données de santé, infraction, 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.

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 numérique.

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.

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.

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 3 registres :

1. un pour le traitement 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
3. un dernier registre spécifique dans lequel doivent être notifié à la CNIL les violations de données personnelles.

Le registre du responsable de traitement

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 des 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 des données
3. les catégories de personnes concernées (clients, prospects, employés, etc, …)
4. les catégories de données personnelles 'exemple : 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

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 2ème 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 1er 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.

Le registre des notifications

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, détruite, 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 de CNIL.

Si ces risques sont élevés pour ces personnes, vous devrez les en informer.

A l'issue de cette étape, vous serez en capacité d'assurer une protection des données personnelle en continu et de faire face aux incidents.

RGPD

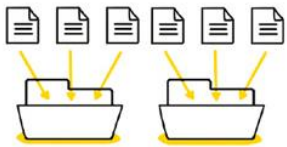
PASSER À L'ACTION

en 4 étapes

1

Constituez un registre de vos traitements de données

2



Faites le tri dans vos données

3

Respectez les droits des personnes

4

Sécurisez vos données

❶ Constituer un registre de vos traitements de données

Ce document vous permet de recenser tous vos fichiers et d'avoir une vision d'ensemble.
Identifier les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données.
Exemple : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc., …

Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :

- L'objectif poursuivi (la finalité – exemple : la fidélisation du client) ;
- Les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire, etc., …) ;
- Qui a accès aux données (le destinataire – exemple : service chargé du recrutement, service informatique, direction, prestataire, partenaire, hébergeurs,) ;
- La durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

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

Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.
En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.

❷ Faites le tri dans vos données

La constitution du registre vous permet de vous interroger sur les données dont votre entreprise a réellement besoin.

Pour chaque fiche de registre créée, 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) ;
- vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter (voir la fiche « Traitements de données à risque : êtes-vous concerné ? ») ;

- seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- vous ne conservez pas vos données au-delà de ce qui est nécessaire.

A cette occasion, améliorez vos pratiques ! Minimisez la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise. Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

❸ Respectez le droit des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

Informez les personnes. A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Vérifiez que l'information comporte les éléments suivants :

- pourquoi vous collectez les données (« la finalité » ; par exemple pour gérer l'achat en ligne du consommateur) ;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
- Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;
- Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle ») ;
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
- Si vous transférez des données hors de l'UE (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez par exemple, donner un premier niveau d'information en fin de

formulaire et renvoyer à une **politique de confidentialité / page vie privée** sur votre site internet.

À l'issue de cette étape, vous avez répondu à votre obligation de transparence.

Permettez aux personnes d'exercer facilement leurs droits
Les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

Vous devez leur donner les moyens d'exercer effectivement leurs droits. Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez à vos clients la possibilité d'exercer leurs droits à partir de leur compte.

Mettez en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

BONNE PRATIQUE : SOYEZ REACTIFS !
Bien traiter les demandes des consommateurs quant à leurs données personnelles c'est :

- renforcer la confiance qui sécurise la relation-client ;
- vous mettre à l'abri de critiques sur les réseaux sociaux, ou de réclamations auprès de la CNIL.

A l'issue de cette étape, vous serez en capacité de répondre aux demandes des personnes concernées.

❹ Sécurisez vos données

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour garantir au mieux la sécurité des données. Vous êtes en effet tenu à une obligation légale d'assurer la sécurité des données personnelles que vous détenez.

Vous garantissez ainsi l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d'incident.

Des réflexes doivent être mis en place : 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.

EXEMPLE DE REGISTRE

Pour faciliter la tenue du registre, la CNIL propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.

Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre organisme en tant que responsable de traitement. Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévue par le RGPD.

Une fois ce recensement effectué, vous serez en mesure de procéder à l'analyse des traitements de données personnelles à la réglementation.

Composition du document

1. La page 2 du registre recense les informations communes à toutes vos activités de traitement.

- Les coordonnées de votre organisme (ou de son représentant sur le territoire européen si votre organisme n'est pas établi dans l'Union européenne).
- Les coordonnées du délégué à la protection des données (DPO) si vous en disposez.
- La liste des activités de votre organisme impliquant le traitement de données personnelles.

2. Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre (page 3 à 6).

Les pages suivantes constituent le modèle de fiche de registre, que vous devrez remplir pour chacune de ces activités.

REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	Nom : Prénom Adresse : CP : Ville : Téléphone : Adresse de messagerie :
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	Nom : Prénom Adresse : CP : Ville : Téléphone : Adresse de messagerie :

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités
Activité 1	ex. Gestion de la paie
Activité 2	ex. Gestion des prospects
Activité 3	ex. Gestion des fournisseurs
Activité 4	ex. Vente en ligne
Activité 5	ex. Sécurisation des locaux
Activité 6	ex. …
Activité 7	ex. …
Activité 8	ex. …

Vous devez créer et tenir à jour une fiche de registre par activité.

Le modèle de fiche de registre est disponible sur la page suivante, copier/coller autant de fois la sélection qu'il y a d'activité listées.

----> Début de section à copier pour chaque activité listée en page 2 <----

FICHE DE REGISTRE DE L'ACTIVITÉ

Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de données est partagée avec un autre organisme)*	
Nom du logiciel ou de l'application *(si pertinent)*	

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.
Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1.
2.
3.
4.

Catégories de données collectées

Cochez et listez les différentes données traitées

☐ État-civil, identité, données d'identification, images (ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)

☐ Vie personnelle (ex. habitudes de vie, situation familiale, etc.)

☐ Vie professionnelle (ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)

☐ Informations d'ordre économique et financier (ex. revenus, situation financière, données bancaires, etc.)

☐ Données de connexion (ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

☐ Données de localisation (ex. déplacements, données GPS, GSM, …)

☐ Internet (ex. cookies, traceurs, données de navigation, mesures d'audience, …)

☐ Autres catégories de données (précisez) :

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et 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).

☐ Oui ☐ Non

Si oui, lesquelles ? :

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Jours, Mois, Ans, Autre durée :

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. 2.
3. 4.

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. 2.
3. 4.

Sous-traitants
(Exemples : hébergeurs, prestataires de maintenance informatique, etc.)

1. 2.
3. 4.

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☐ Non

Si oui, vers quel(s) pays :

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☐ Contrôle d'accès des utilisateurs
Décrivez les mesures :

☐ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs)*, les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

☐ Mesures de protection des logiciels *(antivirus, mises à jour et correctifs de sécurité, tests, etc.)*
Décrivez les mesures :

☐ Sauvegarde des données
Décrivez les modalités :

☐ Chiffrement des données
Décrivez les mesures (exemple : site accessible en https, utilisation de TLS, etc.) :

☐ Contrôle des sous-traitants
Décrivez les modalités :

☐ Autres mesures :

----> Fin de section à copier pour chaque activité listée en page 2 <----

cpme 71
SAÔNE-ET-LOIRE

31, rue Denon - 71100 Chalon-sur-Saône
03.85.42.96.44
administration@cpme-71.fr