

Guide de sensibilisation au RGPD

POUR LES ORGANISATIONS
SYNDICALES

PRO

Sommaire

Sommaire	2
Avant-propos	3
Introduction	4
Les grandes notions « Informatique et Libertés »	5
Fiche n° 1 : Pour quels objectifs votre organisation syndicale peut-elle être amenée à traiter des informations personnelles ?	6
Fiche n° 2 : Qui est responsable des données lorsqu'un traitement est mis en place ?	9
Fiche n° 3 : Comment s'assurer que votre traitement d'informations personnelles est permis ?	14
Fiche n° 4 : Quelles informations personnelles peuvent être collectées par votre organisation syndicale ?	18
Fiche n° 5 : Quelles précautions prendre lorsque votre organisation syndicale traite des informations révélant les opinions syndicales ou d'autres informations sensibles (santé, orientation sexuelle, condamnation pénale, etc.) ?	21
Fiche n° 6 : À quel organisme votre organisation syndicale peut-elle transmettre des informations ?	24
Fiche n° 7 : Pendant combien de temps votre organisation syndicale peut-elle conserver des informations personnelles ?	26
Fiche n° 8 : Comment informer les personnes concernées des traitements mis en place ?	30
Fiche n° 9 : Quelles mesures votre organisation syndicale doit-elle prendre pour garantir les droits des personnes concernées ?	33
Fiche n° 10 : Une organisation syndicale doit-elle effectuer des formalités avant de mettre en place un traitement ?	37
Fiche n° 11 : Comment sécuriser les informations personnelles traitées et ne les communiquer qu'aux personnes autorisées ?	42
Fiche n° 12 : Quelles précautions prendre lors du choix des outils de votre organisation syndicale ?	45
Glossaire	46

Avant-propos

Dans le cadre de leur mission de défense des intérêts collectifs des travailleurs, les organisations syndicales sont amenées à recueillir des informations relatives à des personnes physiques telles que des salariés, des adhérents ou encore des sympathisants.

Une mauvaise gestion de ces informations personnelles peut s'avérer extrêmement préjudiciable pour les personnes concernées, susceptibles de devoir faire face à des répercussions professionnelles et personnelles importantes.

Afin de ne pas altérer le contrat de confiance existant entre l'organisation syndicale et les personnes en lien avec celle-ci, des mécanismes permettant de protéger les informations personnelles traitées doivent être mis en place ainsi qu'une « *gestion éthique* » de ces informations. Cela constitue également une obligation légale.

La réglementation a en effet vocation à protéger les informations personnelles des citoyens afin que ces dernières ne soient pas utilisées et divulguées plus que nécessaire. Cela signifie qu'un organisme, lorsqu'il utilise ces informations, doit veiller à respecter certains principes pour ne pas porter atteinte au droit au respect de la vie privée.

Afin d'aider les organisations syndicales de salariés à s'appropriier ces règles, la CNIL a choisi de proposer un guide permettant de mettre en œuvre concrètement, et le plus en amont possible, les principes « Informatique et Libertés ».

Précisions lexicales

Dans ce guide, est entendu par :

- « **organisation syndicale** », la structure à laquelle appartient le lecteur du guide ;
- « **entité** », une structure appartenant au mouvement par exemple, une section locale, une confédération, une fédération ;
- « **mouvement** », l'ensemble des entités d'un même syndicat ;
- « **personnes concernées** », les adhérents, sympathisants, salariés et toute autre personne dont les informations sont traitées ».

Introduction

Le règlement européen sur la protection des données (RGPD) et la loi Informatique et Libertés définissent des règles s'imposant à tout organisme qui utilise des informations personnelles.

La mise en place de ces règles suppose :

- de comprendre les missions de la CNIL, notamment en matière d'accompagnement des organismes ;
- d'identifier les acteurs susceptibles de vous aider ;
- de s'assurer de votre bonne compréhension de certaines notions centrales.

L'accompagnement de la CNIL

Si la CNIL est avant tout connue pour être l'autorité de contrôle des règles relatives à la protection des informations personnelles, elle a à cœur sa mission d'accompagnement des professionnels.

L'article 8 de la loi Informatique et Libertés prévoit que la CNIL « *conseille les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel* ».

Pour cela, elle élabore des instruments tels que des référentiels, des guides pratiques ou des recommandations à destination des usagers. [Ils sont librement accessibles sur son site web *cnil.fr*](#).

Elle met également à disposition un MOOC présentant de manière dynamique le RGPD. Vous y trouverez l'ensemble des informations pour vous initier au RGPD et débiter ainsi la mise en conformité de votre organisation syndicale.

Pour aller plus loin

- [Les missions de la CNIL](#) sur *cnil.fr*
- [Statut et organisation de la CNIL](#) sur *cnil.fr*

Le délégué à la protection des données, le référent de votre organisme en matière de protection des informations personnelles

La désignation d'un référent ou délégué à la protection des données (DPD ou DPO pour *Data Protection Officer*), chargé de piloter l'application des règles relatives à la protection des informations personnelles au sein d'une structure, revêt un caractère obligatoire pour la plupart des organisations syndicales.

Il est principalement en charge :

- **d'informer et de conseiller les organismes qui utilisent des informations personnelles ;**
- **de s'assurer du respect des règles** en matière de protection des informations personnelles ;
- **de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci.

Pour aller plus loin

- Le [délégué à la protection des données \(DPO\)](#) sur *cnil.fr*

Les grandes notions « Informatique et Libertés »

La consultation des différentes fiches de ce guide suppose pour le lecteur de bien comprendre certaines notions essentielles.

Qu'est-ce qu'une information personnelle ?

Une information personnelle est une information se rapportant à une personne physique qui peut être identifiée :

- directement (exemple : nom et prénom) ;
- ou indirectement (exemple : un numéro d'adhérent, un numéro de téléphone ou de plaque d'immatriculation, le numéro de sécurité sociale, une adresse courriel, mais aussi la voix ou l'image).

ATTENTION

L'identification d'une personne physique peut être réalisée par un croisement d'un ensemble d'informations détenues par votre organisation syndicale ou par un tiers.

Par exemple, une enquête par questionnaire auprès des adhérents peut, même lorsque les noms et prénoms ne sont pas indiqués, contenir des réponses qui, combinées les unes aux autres, peuvent permettre de retrouver l'identité de l'adhérent concerné. Ainsi, la collecte des informations relatives à l'âge, au sexe, à la section syndicale est susceptible de révéler l'identité d'une personne.

En revanche, des coordonnées d'un syndicat (par exemple, « syndicatA@email.fr ») ne sont pas des informations personnelles.

Qu'est-ce qu'un traitement d'informations personnelles ?

Toute utilisation d'informations personnelles constitue un « traitement », quel que soit le procédé utilisé : collecte, enregistrement, conservation, consultation, utilisation, communication, etc.

C'est donc une notion très large : tout maniement d'informations personnelles, y compris une simple consultation, est un « traitement » d'informations personnelles.

Par exemple, constituent des traitements d'informations personnelles :

- l'installation d'un système de vidéosurveillance au sein de votre organisation syndicale ;
- la création d'un tableau Excel qui regroupe l'ensemble des actions effectuées auprès des adhérents ;
- la diffusion d'un formulaire de collecte d'informations personnelles sur votre site web.

ATTENTION

Un traitement d'informations personnelles n'est pas nécessairement informatisé : les **fichiers papier** sont également concernés et doivent être protégés dans les mêmes conditions.

Qu'est-ce qu'une finalité ?

Il s'agit de la **raison d'être**, de l'**objectif poursuivi** par l'organisation syndicale lorsqu'elle utilise des informations personnelles.

La gestion administrative des adhérents et sympathisants et la gestion de la lettre d'information de votre organisation syndicale constituent par exemple deux finalités distinctes et deux traitements différents.

Pour plus de définitions, consultez le [glossaire](#) de ce guide.

Fiche n° 1 : Pour quels objectifs votre organisation syndicale peut-elle être amenée à traiter des informations personnelles ?

Règles de droit

Votre organisation syndicale ne peut collecter des informations personnelles que pour **poursuivre un objectif** (également appelé « finalité »). Cet objectif, c'est-à-dire ce à quoi vont servir les informations personnelles, doit être **défini avant** de mettre en œuvre le traitement

Pour être conforme au RGPD, cet objectif doit répondre à **trois critères**. On dit qu'il doit être **déterminé, explicite et légitime**.

• Il doit être déterminé en amont

L'objectif du traitement doit être défini avant la mise en place du traitement. En découleront :

- **la nature et l'étendue des informations pouvant être collectées ainsi que le moment de la collecte** : seules les informations adéquates et strictement nécessaires pour atteindre l'objectif prévu pourront être collectées (*Pour plus d'informations, consultez [la fiche n° 4](#) du guide relative à la pertinence des informations collectées*) ;
- **la durée de conservation des informations traitées** : en fonction de l'objectif du traitement, les informations collectées pourront être conservées plus ou moins longtemps. Par exemple, on ne conservera pas pour la même durée des informations traitées dans le cadre de l'envoi d'une lettre d'information ou de la gestion des adhérents.

Exemple d'objectif ne pouvant pas être considéré comme déterminé :

Si une organisation syndicale se contente d'informer l'adhérent que « *le traitement est mis en œuvre à des fins d'intérêt légitime de l'organisme* », il ne s'agit pas d'un objectif déterminé puisqu'il ne définit pas ce à quoi va servir le traitement.

• Il doit être explicite

Tout traitement doit avoir un objectif explicite, c'est-à-dire énoncé en **des termes clairs, simples et compréhensibles**. Il ne doit pas y avoir de buts cachés.

Ainsi, vous devez **expressément indiquer ce pourquoi vous collectez des informations personnelles** quand bien même cet objectif pourrait être considéré comme évident.

Dans un souci de transparence, l'objectif du traitement doit être **porté à la connaissance de la personne concernée pour lui permettre de comprendre la raison de la mise en place du fichier**. La personne concernée doit ainsi être en mesure de savoir quelles sont les utilisations possibles de ses informations personnelles par votre organisation syndicale dans le cadre des traitements déployés. (*Pour plus d'informations, consultez la [fiche n° 8](#) du guide relative à l'information des personnes concernées*).

À NOTER

L'objectif du traitement est une information qui doit **nécessairement figurer dans le registre des traitements, c'est-à-dire dans la liste détaillée des fichiers**. (*Pour plus d'informations, consultez la [fiche n° 10](#) du guide relative aux formalités préalables*).

• Il doit être légitime

La légitimité d'un objectif de traitement s'apprécie par rapport à l'ensemble de la législation applicable au traitement mis en place.

Un objectif de traitement ne sera donc pas légitime s'il porte notamment atteinte à une réglementation, à un principe général de droit ou encore à une liberté fondamentale.

Par exemple, la réalisation par votre organisation syndicale d'une enquête auprès de l'**ensemble** de ses salariés afin de collecter des informations sur leur opinion sur l'action du syndicat, n'apparaît a priori pas légitime puisque cela constitue une atteinte à la vie privée. Toutefois, de telles données peuvent être demandées à certains candidats au stade du recrutement, dès lors que le poste pour lequel ils candidatent participe à la représentation idéologique du mouvement, à la détermination de son éthique ou de son programme.

À l'inverse, **on peut présumer qu'un objectif est légitime dès lors que le traitement est mis en place pour répondre à une obligation légale.**

En pratique

Les objectifs des traitements mis en place par votre organisation syndicale sont multiples. Il peut notamment s'agir de :

- gestion des adhérents et sympathisants :
 - gestion administrative des adhérents ;
 - gestion des cotisations ;
 - gestion des fichiers d'adhérents et de sympathisants ;
- gestion des activités organisées et services proposés par le syndicat :
 - gestion des informations relatives aux activités et événements du syndicat ;
 - lettre d'information ;
 - gestion des formations ;
 - assistance juridique ;
- gestion du fonctionnement administratif du syndicat : gestion des instances statutaires ;
- gestion du personnel : gestion du recrutement ;
 - gestion administrative des personnels ;
 - gestion des rémunérations et accomplissement des formalités administratives afférentes ;
 - mise à disposition d'outils professionnels ;
 - organisation du travail ;
 - suivi des carrières et de la mobilité ;
 - gestion des formations ;
 - tenue des registres obligatoires ;
 - rapports avec le CSE ;
 - communication interne ;
 - gestion des aides sociales ;
 - réalisation des audits ;
 - gestion du contentieux et du précontentieux ;
- gestion des prestataires : gestion et suivi des contrats de fourniture de biens et de prestation de services.

Quelles sont les conditions à la réutilisation des informations personnelles pour un objectif différent de celui initialement prévu ?

L'objectif ayant conduit à la collecte des informations personnelles des adhérents et salariés **doit être respecté tout au long de l'utilisation de celles-ci**. Toutefois, un objectif est susceptible d'évoluer au fil du temps, sous réserve du respect de certaines conditions.

Si vous souhaitez réutiliser des informations en votre possession pour un objectif différent de celui initialement prévu, vous devez vous assurer que **ce nouvel objectif est compatible avec l'objectif initial**.

Pour savoir si un objectif ultérieur est compatible avec la raison première de la mise en place du traitement, vous devez effectuer une **analyse de compatibilité**. Cette analyse doit prendre en compte les éléments suivants :

- l'existence d'un lien éventuel entre l'objectif du traitement initial et celui du traitement ultérieur envisagé ;
- le contexte dans lequel les informations personnelles sont collectées ;
- la nature des informations traitées (en particulier si le traitement porte sur des catégories particulières d'informations personnelles) ;
- les conséquences possibles du traitement ultérieur des informations pour les personnes concernées ;
- les garanties mises en place pour assurer la sécurité des informations (par exemple le chiffrement des informations ou la pseudonymisation).

Exemple : une organisation syndicale décide de transmettre son fichier d'adhérents à un organisme complémentaire de santé

Les informations ont été collectées et traitées pour répondre à un objectif d'enregistrement des adhésions et l'organisation syndicale souhaite transmettre ces mêmes informations à des organismes complémentaires de santé afin de proposer leurs services à leurs adhérents. L'objectif ultérieur n'apparaît pas compatible avec la raison initiale de mise en place du fichier. En effet, les personnes concernées avaient communiqué leurs informations dans l'objectif d'adhérer à un mouvement et cela ne préjuge pas de leur souhait de recevoir des informations relatives à des organismes complémentaires de santé.

ATTENTION

En cas de réutilisation des informations personnelles pour un objectif ultérieur qui serait compatible avec l'objectif initial, votre organisation syndicale devra s'assurer d'**informer la personne concernée** avant la mise en place du traitement ultérieur et celle-ci devra être en mesure de s'y opposer.

Pour se mettre en conformité :

- s'assurer que tous vos traitements disposent d'un objectif **déterminé, explicite et légitime** ;
- vérifier que les informations collectées pour répondre à cet objectif **ne sont pas réutilisées pour répondre à un autre objectif**, sauf à ce que cette réutilisation soit compatible avec l'objectif initial et à la condition d'en avoir informé la personne concernée ;
- dans le cadre de l'analyse de compatibilité entre deux objectifs, documenter **votre démarche** afin d'être en mesure de la justifier.

Références

- [Articles 5 et 6.4 du RGPD sur cnil.fr](#)
- [Article L. 1133-1 du code du travail sur légifrance.fr](#)

Fiche n° 2 : Qui est responsable des données lorsqu'un traitement est mis en place ?

Règle de droit

Le RGPD prévoit trois statuts possibles pour les acteurs qui utilisent des informations personnelles : **responsable des données** (également appelé « responsable de traitement »), responsable conjoint des données et sous-traitant. La détermination de ce statut permettra de connaître les obligations de chacun.

Une entité est **responsable des données** lorsqu'elle détermine l'objectif et les caractéristiques du traitement (nature des informations collectées, durée de conservation des informations, mesures de sécurité mises en place, etc.). Le responsable des données est, sauf désignation par un texte législatif ou réglementaire, l'organisme qui décide de la création du traitement. Il définit ainsi le « *pourquoi* » et le « *comment* » du traitement et dispose d'un réel pouvoir décisionnel.

Les entités sont **responsables conjoints des données si elles déterminent conjointement les objectifs et les moyens d'un même traitement**. Dans une telle situation, un accord doit être conclu entre les entités afin de définir de manière transparente le rôle et les obligations de chacun en ce qui concerne la conformité du traitement aux exigences du RGPD.

Un organisme dispose du **statut de sous-traitant lorsqu'il traite des informations personnelles pour le compte, sur instruction et sous l'autorité d'un responsable des données**. Un contrat ou un autre acte juridique devra être établi afin de préciser les obligations de chacun en ce qui concerne l'objet, la durée, la nature et l'objectif du traitement, les catégories d'informations collectées sur les travailleurs, etc.).

La ligne de partage entre ces trois catégories peut parfois être délicate à fixer. La qualification doit intervenir au terme d'une **analyse concrète des modalités de création et de mise en place des traitements**.

Selon la logique de responsabilisation, c'est aux organismes eux-mêmes de documenter l'analyse ayant conduit à la qualification retenue.

ATTENTION

Cela ne **signifie pas pour autant que les entités peuvent « choisir » la qualification qui les arrange** : elles doivent être en mesure de justifier concrètement la qualification retenue.

L'intérêt principal de la distinction entre responsable des données et sous-traitant réside dans **l'étendue de leurs obligations respectives qu'ils ont l'un envers l'autre, et surtout à l'égard des personnes concernées**. Une répartition erronée des responsabilités n'emporte pas de conséquence particulière si les obligations relatives à la protection des informations personnelles ont été respectées. Le tableau qui suit présente les obligations principales qui pèsent sur chacune des parties.

Nature des obligations	Articles RGPD	Responsable des données	Sous-traitant	Co-responsable des données
Rédiger un écrit précisant les obligations respectives de chacun des acteurs	26 ; 28	✓	✓	✓
Documenter les instructions du responsable des données concernant les traitements des informations personnelles par le sous-traitant		✓	✓	✓
Obtenir et conserver une autorisation écrite préalable du responsable des données pour recourir aux services d'un sous-traitant	28	✗	✓	✗
Tenir le registre des traitements mis en place	30	✓	✓	✓
Réaliser une analyse d'impact (en cas de réalisation des critères du RGPD)	35	✓	✗	✓
Informers les autres acteurs du traitement (responsable des données, sous-traitant et co-responsable des données) en cas de soupçon de violation du RGPD	28	✗	✓	✗
Informers la CNIL et/ou les personnes concernées en cas de violation des informations personnelles	33 ; 34	✓	✗	✓
Fournir aux personnes concernées les informations obligatoires	12 à 14	✓	✗	✓
Traiter les demandes d'exercice de droits (accès, effacement, opposition, etc.)	15 à 23	✓	✗	✓
Assister le responsable des données dans le traitement de telles demandes	28	Sans objet	✓	✗

En pratique

Les mouvements syndicaux sont structurés selon un schéma faisant intervenir différentes entités : syndicats, unions locales et départementales, comités régionaux, fédérations, confédérations, etc.

La détermination des différentes responsabilités entre les entités n'est pas figée : chacune des entités peut avoir un rôle différent en fonction de la nature du traitement mis en place.

Dans la mesure où la gestion des adhésions représente un traitement central pour les organisations syndicales, les éléments suivants portent principalement sur cet objectif de traitement.

Dans quels cas votre organisation syndicale agit-elle en tant que responsable des données pour la gestion des adhésions ?

L'entité qui définit l'objectif et les caractéristiques du traitement relatif à la gestion des adhésions est considérée comme étant le responsable des données, qu'il s'agisse de la confédération, de l'union locale, régionale ou de la section nationale.

Par exemple, si une union locale gère un service d'enregistrement des demandes d'adhésion à l'union locale (c'est-à-dire qu'elle s'occupe de l'envoi et de la réception des bulletins d'adhésion et procède à l'enregistrement des informations personnelles des adhérents dans une base de données dont elle détermine les personnes

habilités à y accéder et les mesures de sécurité afférentes), alors elle agit en tant que responsable des données pour la gestion des adhésions.

À l'inverse, si c'est la confédération qui se charge de ce traitement alors elle sera considérée comme responsable des données pour la gestion des adhésions.

ATTENTION

Si votre organisation syndicale décide concrètement « pourquoi » et « comment » les informations personnelles sont traitées, **elle doit être considérée comme responsable des données même si elle est désignée comme sous-traitant dans un contrat.**

Les autorités de contrôle ne sont pas liées par la répartition des rôles choisie par les parties et une requalification, appréciée au regard des conditions réelles de mise en place du traitement, est donc toujours possible.

Dans quels cas votre organisation syndicale peut-elle être responsable conjointe des données pour la gestion des adhésions ?

En pratique, la responsabilité conjointe est caractérisée :

- soit parce qu'une **décision commune est prise** par les responsables conjoints concernant l'objectif et les moyens du traitement ;
- soit parce que des **décisions convergentes, complémentaires et nécessaires** sont prises par les responsables conjoints en ce qui concerne l'objectif et les caractéristiques du traitement mis en œuvre. Le traitement ne serait donc pas possible sans la participation des responsables conjoints.

Exemples

Si deux sections locales décident ensemble de mettre en œuvre une plateforme de gestion des adhésions, alors ces entités agissent en tant que responsables conjoints.

De la même manière, si votre organisation syndicale mutualise la mise en œuvre d'un traitement avec d'autres organisations syndicales dans le cadre d'un syndicat de site, l'ensemble de ces organisations syndicales endossent le rôle de responsables conjoints.

Néanmoins, toute entité ou prestataire influant sur le traitement mis en place n'est pas nécessairement responsable conjoint des données. Tout dépendra du rôle joué par l'organisme dans la décision de créer le traitement et la définition des moyens et des conditions de mise en place de celui-ci. Une entité peut être considérée comme responsable des données même si elle n'accède pas aux informations personnelles.

L'existence d'une responsabilité conjointe n'implique pas nécessairement des responsabilités équivalentes entre les responsables des données.

À NOTER

Le partage des responsabilités entre les organismes ne doit pas avoir de conséquences pour les personnes concernées. Ces dernières doivent ainsi pouvoir exercer leurs droits auprès de chacun des responsables conjoints, peu important le contenu de l'accord conclu entre ceux-ci.

Dans quels cas un organisme est-il sous-traitant pour la gestion des adhésions ?

Un organisme est sous-traitant lorsqu'il agit pour le compte et sur instruction du responsable des données, même si une marge de manœuvre peut lui être laissée pour prendre certaines décisions (par exemple, lorsque le responsable des données laisse le sous-traitant définir les moyens techniques et organisationnels les plus appropriés).

Exemple

Si votre organisation syndicale, responsable des données, confie à un prestataire externe la conception et l'hébergement de votre site web au sein duquel vos adhérents disposent d'un espace personnel dédié, alors ce prestataire agit en tant que sous-traitant et votre organisation syndicale en tant que responsable des informations collectées à des fins de conception et d'hébergement du site web.

Les activités d'un sous-traitant peuvent également concerner des tâches plus précises telles que la relance des adhérents et des sympathisants dans le cadre des élections professionnelles.

À NOTER

Une distinction doit être faite entre la notion de prestataire de services et celle de sous-traitant : tous les prestataires de services ne sont pas nécessairement sous-traitants au sens du RGPD, une analyse au cas par cas est nécessaire.

À titre d'exemple, la société effectuant une prestation de ménage dans les locaux de votre organisation syndicale ou le graphiste chargé de concevoir les éléments graphiques de votre site web sont des prestataires de service. Ils ne peuvent toutefois pas être qualifiés de sous-traitants dans la mesure où ils ne traitent pas d'informations personnelles pour le compte de votre organisation syndicale. La nature du service effectué par le prestataire auquel fait appel le responsable des données permet ainsi de donner des indices pour retenir ou non la qualification de sous-traitant.

Schéma de synthèse : quel statut appliquer aux différentes structures des organisations syndicales ?

Quel statut pour les organisations syndicales ?

1

RESPONSABLE DES DONNEES

Définition :

il détermine les objectifs et les moyens du traitement.



Questions à se poser:

- L'entité a-t-elle décidé de la création du traitement ?
- A-t-elle défini le « pourquoi » et le « comment » ?
- Dispose-t-elle d'un pouvoir décisionnel ?

2

RESPONSABLES CONJOINTS DES DONNEES

Définition :

ils déterminent conjointement les objectifs et les moyens d'un même traitement.



Questions à se poser:

- Une décision commune est-elle prise par les responsables conjoints concernant l'objectif et les moyens du traitement ?
- Des décisions convergentes, complémentaires et nécessaires sont-elles prises par les responsables conjoints concernant l'objectif et les moyens du traitement ?
- Le traitement est-il possible sans la participation des deux responsables conjoints de traitement identifiés ?

3

SOUS-TRAITANT

Définition :

il traite des informations personnelles pour le compte, sur instruction et sous l'autorité d'un responsable des données.



Questions à se poser:

- Le service fourni intervient-il à la demande du responsable des données ?
- Le service suppose-t-il le traitement d'informations personnelles par le prestataire ?
- Un contrôle est-il réalisé par le responsable des données ? Quelle en est l'étendue ?

Pour se mettre en conformité :

- **effectuer une analyse approfondie de la responsabilité de chacune des entités de votre organisation syndicale** (syndicats, unions locales, fédérations professionnelles, confédération, etc.) intervenant dans le traitement des informations personnelles, depuis leur collecte jusqu'à leur suppression ;
- **tracer**, dans les supports de documentation interne, **la réflexion menée et la justification retenue** pour déterminer le statut des acteurs ;
- **établir des supports juridiques** (statuts, conventions, chartes, contrats, etc.) afin de clarifier et de déterminer les rôles et les obligations de chacun ;
- **informer** les personnes concernées de l'identité du responsable des données afin qu'elles puissent exercer leurs droits ;
- pour être accompagné dans l'analyse du statut de l'acteur concerné, **échanger avec le délégué à la protection des données** (DPO) de l'organisme (s'il dispose d'un DPO).



Références

- [Articles 4, 26, 28](#) du RGPD sur [cnil.fr](#)
- [Lignes directrices du CEPD du 2 septembre 2020 sur les notions de responsable de traitement et de sous-traitant](#) (en anglais) sur [edps.europa.eu](#)
- [Guide du sous-traitant](#) de la CNIL sur [cnil.fr](#)

Fiche n° 3 : Comment s'assurer que votre traitement d'informations personnelles est permis ?

Règles de droit

Un traitement doit être **licite, c'est-à-dire permis par le droit**, cela signifie qu'il doit répondre à deux critères :

- son **objectif doit être conforme au droit** (par exemple, un traitement de données ne peut pas avoir pour objectif une discrimination illégale) ;
- il doit reposer sur **l'une des six « bases légales »** prévues par le RGPD, c'est-à-dire l'une des conditions permettant de mettre en place le traitement.

Cette condition ou « base légale » doit être déterminée **avant la mise en place du traitement et être portée à la connaissance de la personne concernée** dans la mesure où elle conditionne la **possibilité d'exercer certains droits**. *Pour plus d'informations, consultez les [fiches n°8](#) et [9](#) du guide.*

Il vous appartient donc de déterminer une condition/base légale pour **chaque objectif de traitement**.

À NOTER

Plusieurs conditions/bases légales peuvent parfois s'avérer appropriées pour justifier un traitement. Vous êtes libres de choisir celle qui vous semble la plus appropriée au regard de l'objectif poursuivi par votre traitement : il n'est en effet pas possible de retenir plusieurs bases légales. Vous devrez également documenter les raisons qui justifient votre choix.

ATTENTION

La condition/base légale fondant le traitement doit être distinguée de l'exception permettant de traiter des informations sensibles, dont le traitement est par principe interdit. *Pour plus d'informations sur les informations sensibles, nous vous invitons à consulter [la fiche n° 5](#) du guide.*

Ainsi, si un traitement porte sur des informations sensibles, votre organisation syndicale doit déterminer la condition/base légale du traitement ainsi que l'exception permettant de lever l'interdiction de traiter ces informations sensibles.

Par exemple, pour mettre en œuvre le traitement relatif à la constitution d'un fichier d'adhérents, votre organisation syndicale doit définir :

- Premièrement, **la condition/base légale du traitement** : en l'occurrence « l'intérêt légitime » poursuivi par votre organisation syndicale ;
- Deuxièmement, **l'exception permettant de traiter des informations sensibles**, en l'occurrence l'appartenance syndicale : « *le traitement est effectué par un organisme à but non lucratif poursuivant une **finalité syndicale et se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités, sous réserve que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées*** ».

En pratique

Dans le cadre des traitements que votre organisation syndicale met en place, vous êtes susceptible d'invoquer les conditions/bases légales suivantes :

Cette condition/base légale peut par exemple fonder les traitements relatifs à la gestion du recrutement des salariés, la gestion des cotisations des adhérents, ou encore l'accompagnement juridique offert aux adhérents dans le cadre d'un contrat d'adhésion.

Le traitement est nécessaire à l'exécution d'un contrat

L'exécution d'un contrat peut justifier la mise en place de traitements (contrat de travail, contrat d'adhésion, etc.).

Le traitement vise à satisfaire un intérêt légitime poursuivi par votre organisation syndicale

Un traitement peut être fondé sur la réalisation d'un intérêt légitime poursuivi par votre organisation syndicale, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux des personnes concernées.

Cela signifie que votre organisation syndicale doit trouver **un équilibre pour atteindre son objectif considéré comme légitime tout en veillant à ne pas porter une atteinte disproportionnée aux droits des personnes concernées** (salariés, adhérents ou sympathisants).

Le choix de cette condition/base légale suppose de définir précisément l'intérêt légitime poursuivi et de trouver un équilibre entre les intérêts de chacune des parties en analysant notamment :

- les **conséquences** que le traitement est susceptible d'emporter **pour la personne concernée** ;
- les **attentes raisonnables de la personne concernée** c'est-à-dire le fait qu'elle s'attende à ce que ce traitement soit mis en place par le responsable des données.

Exemples

La réalisation de statistiques pour étudier la population adhérant à votre organisation syndicale peut être fondée sur l'intérêt légitime de votre entité dans la mesure où ce traitement ne porte pas une atteinte disproportionnée aux droits des personnes concernées (les informations ne font pas l'objet d'une communication à l'extérieur, seul le personnel habilité accède aux informations traitées, etc.).

De la même façon, l'envoi d'un bulletin d'information aux adhérents peut reposer sur l'intérêt légitime. Votre organisation syndicale est en effet légitime à communiquer sur ses actions à venir ou passées auprès des personnes ayant décidé d'adhérer.

À NOTER

La nature de l'intérêt légitime poursuivi par votre organisation syndicale devra être portée à la connaissance des personnes concernées dans la mention d'information. *Pour plus d'informations, consultez la [fiche n° 8 du guide](#).*

Celles-ci devront par ailleurs être en mesure de s'opposer à ces traitements.

Il existe une obligation légale qui justifie la mise en place du traitement

Un traitement peut être fondé sur le respect d'une obligation légale dès lors que sa mise en place est rendue obligatoire, de façon suffisamment précise, par un texte législatif ou réglementaire.

Par exemple, une organisation syndicale est dans l'obligation d'effectuer une déclaration sociale nominative pour chacun de ses salariés afin de se conformer aux dispositions du code de la sécurité sociale. Les caractéristiques du traitement et notamment la nature des informations devant être communiquées sont précisément encadrées par les textes. Dans ces conditions, le respect d'une obligation légale apparaît être la condition/base légale opportune pour ce traitement.

ATTENTION

Les dispositions légales doivent être suffisamment précises pour fonder un traitement sur cette condition/base légale. Ainsi, si la législation impose à l'employeur le versement d'une rémunération au travailleur, cette obligation n'est pas suffisamment précisée dans les textes pour que le traitement de gestion de la paye soit fondé sur l'obligation légale.

La personne concernée a donné son accord pour que ses informations soient traitées (consentement)

L'accord recueilli doit être **libre, explicite et éclairé**. Cela signifie que :

- elle l'accepte sans contrainte et est libre de changer d'avis ;
- l'accord qu'elle donne est clair et sans équivoque ;
- la personne concernée doit comprendre le traitement qui lui est proposé.

En savoir plus

[Conformité RGPD : comment recueillir le consentement des personnes ? sur cnil.fr](#)

L'accord de la personne concernée peut par exemple fonder le traitement relatif à l'envoi de la lettre d'information aux personnes non adhérentes qui ont fait la démarche volontaire de s'inscrire afin de la recevoir.

ATTENTION

En raison du déséquilibre manifeste existant entre un salarié et son employeur, la condition/base légale de l'accord de la personne concernée doit être invoquée avec prudence pour les traitements de gestion des ressources humaines. L'accord doit en effet être libre : cela signifie que les salariés doivent être réellement libres d'accepter ou de refuser le traitement en question, sans que cela entraîne de conséquences pour eux.

Afin d'aider les organisations syndicales dans leur choix de base légale, la CNIL propose, à titre indicatif, un choix de base légale pour chaque objectif de traitements susceptible d'être mis en œuvre dans le cadre de vos activités.

Activités de traitement	Objectifs	Bases légales proposées
Gestion des adhérents et sympathisants	Gestion administrative des adhérents	Intérêt légitime
	Gestion des cotisations d'adhésion	Exécution du contrat
	Gestion du fichier de contacts des sympathisants	Intérêt légitime
Gestion des services proposés par l'organisation syndicale aux adhérents	Gestion de la formation économique, sociale et syndicale	Intérêt légitime
	Mise en relation des adhérents avec des avocats spécialisés	Intérêt légitime
	Envoi de bulletins d'informations	Intérêt légitime
Communication auprès des non-adhérents	Envoi de lettres d'information aux personnes ayant demandé à la recevoir	Accord de la personne concernée
Gestion des prestataires	Gestion et suivi des contrats de fourniture de biens et de prestation de services	Exécution du contrat
Gestion du personnel	Recrutement des personnels (collecte d'informations auprès d'un candidat pour évaluer sa capacité à occuper un emploi et mesurer ses aptitudes professionnelles)	Exécution du contrat
	Gestion du dossier professionnel des salariés	Exécution du contrat
	Etablissement des rémunérations, mise à disposition des bulletins de salaire	Exécution du contrat
	Déclaration sociale nominative	Obligation légale
Soutien financier aux adhérents	Gestion de la caisse de grève	Accord de la personne concernée / Exécution du contrat selon les clauses du contrat d'adhésion
	Gestion des remboursements des frais avancés par les adhérents ou militants	Intérêt légitime
Gestion financière et budgétaire	Suivi budgétaire	Obligation légale conformément au règlement n° 2018-06 du 5 décembre 2018 relatif aux comptes annuels des personnes morales de droit privé à but non lucratif
	Suivi des contrats	Intérêt légitime
	Gestion d'une base fournisseurs	Intérêt légitime

Pour se mettre en conformité :

- **choisir la condition/base légale fondant la mise en place du traitement et démontrer qu'elle est opportune** (à travers de la documentation, la référence aux articles de loi dans le registre des traitements c'est-à-dire la liste des traitements mis en place par votre organisme, etc.) ;
- indiquer cette condition/base légale dans le **registre des traitements mis en place dans votre organisme**. *Pour plus d'informations, consultez la [fiche n° 10](#) relative aux formalités préalables ;*
- porter cette condition/base légale à la connaissance des personnes concernées dans une **mention d'information**. *Pour plus d'informations, consultez la [fiche n° 8](#) relative à l'information des personnes concernées.*

En cas de traitement reposant sur l'**intérêt légitime** :

- évaluer le **risque d'atteinte pour les personnes concernées** ainsi que **leurs attentes raisonnables** ;
- trouver un **équilibre entre les droits des personnes et l'intérêt de votre organisme**.

Références

- [Article 6 du RGPD](#) sur [cnil.fr](#)
- [Article L. 2145-5 du code du travail](#) sur [légifrance.fr](#)
- [Article R. 243-1 du code de la sécurité sociale](#) sur [légifrance.fr](#)

Fiche n° 4 : Quelles informations personnelles peuvent être collectées par votre organisation syndicale ?

Règle de droit

Votre organisation syndicale doit veiller à ne traiter que les informations **adéquates, pertinentes et strictement nécessaires à l'objectif poursuivi**. C'est la raison pour laquelle il est essentiel de définir l'objectif du traitement avec suffisamment de précision.

Les informations personnelles collectées doivent avoir un lien direct avec l'objectif poursuivi par le traitement.

Cela signifie, par exemple, que lorsqu'un adhérent bénéficie d'un accompagnement juridique de votre organisation syndicale dans le cadre d'un contentieux prud'homal avec son employeur, la personne en charge de cet accompagnement n'a pas à collecter des informations relatives aux collègues de l'adhérent accompagné, dès lors que cette information ne présente aucun lien avec le litige en cause.

Les informations personnelles traitées sont nécessaires à la réalisation de l'objectif du traitement (gestion des adhérents, organisation de l'aide juridique, etc.).

Les salariés ainsi que les éventuels bénévoles doivent veiller à limiter le volume d'informations enregistrées ainsi que leur niveau de détail. Il s'agit d'être le moins intrusif possible dans la vie de la personne concernée et de ne garder que les informations essentielles, d'un niveau de détail approprié au regard des missions poursuivies par votre organisation syndicale. Les informations collectées doivent ainsi être limitées au strict nécessaire.

Exemple : s'il est possible de collecter des informations relatives à la composition familiale de l'adhérent pour déterminer le montant de la cotisation syndicale, la collecte des noms, prénoms et dates de naissance des enfants de l'adhérent n'apparaît en revanche pas nécessaire.

Les informations personnelles ne doivent pas être collectées « au cas où ».

Les informations personnelles ne peuvent pas être collectées pour un éventuel besoin ultérieur. Par exemple, il n'est pas possible de demander des informations lors de l'adhésion en anticipation d'un accompagnement juridique futur.

L'objectif **du traitement doit être déterminé en amont de la collecte des informations**, en ce qu'il permet de déterminer la nature et la précision des informations nécessaires ainsi que le moment de la collecte.

ATTENTION

Votre organisation syndicale doit être d'autant plus vigilante qu'elle est amenée à traiter des **informations révélant l'appartenance syndicale d'une personne**.

Cette information fait l'objet d'une protection toute particulière au même titre que les informations relatives à la santé, la prétendue origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques ou encore la vie sexuelle ou l'orientation sexuelle. Ces informations dites « sensibles » sont en principe interdites de traitement, sauf **exceptions explicitement prévues par les textes**. Pour plus d'informations sur les règles à respecter en cas de recueil d'informations sensibles, consultez la [fiche n° 5](#) du guide.

En pratique

Dans la mesure où la gestion des adhésions constitue un traitement important d'informations pour votre organisation syndicale, les illustrations suivantes se rapportent principalement à cet objectif de traitement.

En ce qui concerne les autres objectifs, les organisations syndicales peuvent être amenées à traiter d'autres informations personnelles, sous réserve que ces dernières soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard de l'objectif poursuivi.

Quelles sont les informations que votre organisation syndicale peut collecter lors d'une procédure d'adhésion ?

Dans le cadre d'une procédure d'adhésion, vous ne pouvez collecter que les informations nécessaires à l'enregistrement de cette adhésion et à la détermination des cotisations.

En conséquence, il apparaît a priori légitime de collecter certaines catégories d'informations relatives aux futurs adhérents, notamment :

- les informations d'identification (par exemple : nom, prénom) ;
- les coordonnées de contact ;
- leur catégorie socio-professionnelle et le poste occupé ;
- l'entreprise ou l'organisme dans lequel le futur adhérent travaille.

En fonction de la méthode de calcul du montant de la cotisation syndicale choisie par votre organisation syndicale, pourront être collectées des informations personnelles complémentaires, telles que les informations relatives aux traitements, salaires ou pensions, à la composition familiale, au temps de travail ou à la durée de l'adhésion.

Toute autre information qui ne serait pas nécessaire à l'enregistrement de l'adhésion d'une personne et au calcul du montant de sa cotisation ne pourra pas être traitée par votre organisation syndicale.

Par exemple, il est interdit de demander à un futur adhérent :

- son numéro de sécurité sociale ;
- des informations relatives aux appartenances syndicales des membres de sa famille ;
- sa nationalité.

Quels sont les justificatifs que votre organisation syndicale peut demander à un adhérent dans le cadre de la gestion des adhésions ?

Certains justificatifs peuvent comporter des mentions, non pertinentes pour votre organisation syndicale. Il est important de noter que la collecte des justificatifs doit suivre la même logique de minimisation que la collecte des informations personnelles.

Exemple

Un **bulletin de paie** contient de nombreuses informations qui ne sont pas utiles pour déterminer le montant des cotisations des adhérents (des renseignements éventuels sur les jours non travaillés en raison d'un arrêt de maladie, d'un événement personnel ou de l'exercice du droit de grève, le numéro de sécurité sociale, les coordonnées bancaires de la personne, etc.). De ce fait, la collecte des bulletins de paie par votre organisation syndicale apparaît **disproportionnée**. **Il ne pourra ainsi être demandé à un futur adhérent de fournir un bulletin de paie** pour calculer le montant de sa cotisation syndicale.

À NOTER

Des informations complémentaires pourront être collectées par votre organisation syndicale dans le cadre d'autres traitements.

Par exemple, lorsqu'un adhérent dispose d'un accompagnement juridique, de nombreuses informations personnelles pourront lui être demandées, en fonction de la problématique rencontrée : bulletins de paie, contrat de travail, lettres adressées par l'employeur, fiche d'évaluation, etc. Dans cette situation également, votre organisation syndicale doit veiller à ne traiter que les informations **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard de l'objectif poursuivi.

Pour se mettre en conformité :

- solliciter l'**avis du délégué à la protection des données** (DPO) de votre organisation syndicale pour les traitements d'informations personnelles liés aux procédures d'adhésion ;
- s'interroger sur la réalité des **besoins qui justifient la collecte** des informations personnelles ;
- veiller à respecter les exceptions permettant la collecte d'**informations sensibles**, et s'assurer de leur caractère strictement nécessaire. *Pour plus d'informations sur la collecte de ces informations, consultez la [fiche n° 5](#) du guide.*



Références

- [Articles 5](#) et [9](#) du RGPD
- [Articles 1^{er}](#) et [6](#) de la loi Informatique et Libertés

Fiche n° 5 : Quelles précautions prendre lorsque votre organisation syndicale traite des informations révélant les opinions syndicales ou d'autres informations sensibles (santé, orientation sexuelle, condamnation pénale, etc.) ?

Règles de droit

Les informations relatives à l'appartenance syndicale d'une personne sont considérées comme des informations **sensibles** au même titre que celles révélant la prétendue origine raciale ou ethnique, les convictions religieuses ou philosophiques, les informations concernant la santé et les informations relatives à la vie ou à l'orientation sexuelle d'une personne.

De l'ordre de l'intime, ces informations font l'objet d'une protection toute particulière. Leur traitement est donc **en principe interdit sauf dans des exceptions prévues par le RGPD**.

De la même manière, les **informations relatives aux infractions et aux condamnations pénales** sont extrêmement protégées. **Par principe interdit**, le traitement de ces informations ne peut être envisagé par les organisations syndicales que dans des situations limitées.

En pratique

Dans quel cadre votre organisation syndicale peut-elle traiter des informations sensibles ?

Votre organisation syndicale est amenée à traiter des informations sensibles. Vous devez alors vous assurer de pouvoir invoquer l'une des exceptions suivantes :

Personnes concernées	Exception pouvant être invoquée par votre organisation syndicale
<p>Votre organisation syndicale traite des informations sensibles relatives aux salariés de votre organisation.</p> <p>Exemples : informations relatives à l'adaptation du poste de travail à la suite d'une préconisation du médecin du travail susceptibles de révéler des éléments sur l'état de santé d'un salarié, déclarations d'accidents du travail, de maladie et d'autres absences ; informations relatives aux convictions syndicales d'un candidat au stade du recrutement, dès lors que le poste proposé participe à la représentation idéologique du mouvement, à la détermination de son éthique ou de son programme.</p>	<p>Le traitement est nécessaire à votre organisation syndicale pour répondre à certaines de ses obligations ou pour exercer ses droits propres en matière de droit du travail, de la sécurité sociale et de la protection sociale.</p>
<p>Votre organisation syndicale traite l'appartenance syndicale de ses adhérents et sympathisants.</p>	<p>Votre organisation syndicale traite l'appartenance syndicale de ses adhérents et sympathisants dans le cadre de ses activités légitimes, à savoir la défense des intérêts des travailleurs, sous réserve d'assurer la sécurité des informations traitées et de respecter les droits des personnes concernées.</p> <p style="text-align: center;">ATTENTION</p> <p>Le recours à cette exception suppose que le responsable des données ne transmette pas d'informations sensibles telles que l'appartenance syndicale, y compris au sein des différentes entités de son mouvement, sans avoir obtenu</p>

Personnes concernées	Exception pouvant être invoquée par votre organisation syndicale
	<p>l'accord préalable de la personne concernée. <i>Pour plus d'informations, consultez la fiche n° 8.</i></p> <p>Par exemple, cela signifie que si les syndicats locaux ou les unions départementales sont responsables des données, ils ne peuvent pas transférer la liste de leurs adhérents à leur fédération sans avoir préalablement obtenu l'accord des adhérents.</p>
<p>Votre organisation syndicale traite des informations sensibles différentes de l'appartenance syndicale dans le cadre de l'accompagnement proposé à certains adhérents.</p> <p>Exemple : aide aux travailleurs sans papiers pour effectuer leurs démarches de régularisation.</p>	<p>La personne concernée a donné son accord pour lever l'interdiction de traiter des informations sensibles la concernant.</p>
<p>Votre organisation syndicale est amenée à collecter des informations sensibles relatives aux adhérents dans le cadre de l'assistance juridique.</p> <p>Exemple : assistance juridique à un adhérent victime de discriminations en raison de son orientation sexuelle.</p>	<p>Le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.</p>

À NOTER

La communication d'informations sensibles à l'extérieur de votre organisation syndicale doit faire l'objet d'une vigilance particulière. *Pour plus d'informations, consultez la [fiche n° 11](#). Comment sécuriser les informations traitées relatives aux membres du syndicat et salariés ?*

Dans quel cadre votre organisation syndicale peut-elle traiter des informations relatives aux infractions et aux condamnations pénales ?

Votre organisation syndicale peut traiter des **informations relatives aux infractions et aux condamnations pénales** uniquement pour la **préparation, l'exercice et le suivi d'une action en justice en tant que victime ou mise en cause, ou pour le compte de ceux-ci**. Elles ne pourront pas être traitées pour d'autres motifs.

Exemple

Les informations relatives aux infractions et aux condamnations pénales ne peuvent être conservées à titre de justifications comptables.

ATTENTION

Quand bien même un adhérent aurait transmis spontanément des informations sensibles ou des informations relatives à des infractions ou à des condamnations pénales le concernant, il vous appartient de les supprimer dès lors que leur collecte n'apparaît pas justifiée et n'est pas susceptible d'entrer dans le cadre des exceptions prévues par le RGPD.

Pour se mettre en conformité :

- répertorier les informations sensibles traitées ;
- vérifier en amont **qu'une exception permet de collecter des informations sensibles** pour chaque traitement envisagé ou mis en œuvre ;
- s'assurer que les informations relatives aux infractions et aux condamnations pénales peuvent effectivement être traitées sur la base d'une exception prévue au RGPD.

Références

- [Articles 9 et 10](#) du RGPD
- [Article 46 de la loi Informatique et Libertés](#)

Fiche n° 6 : À quel organisme votre organisation syndicale peut-elle transmettre des informations ?

Règle de droit

Votre organisation syndicale est tenue de prendre toutes précautions utiles pour **préserver la confidentialité et la sécurité des informations personnelles**, notamment en empêchant des personnes non autorisées d'y accéder.

Le respect de ce principe suppose une **définition précise des personnes pouvant accéder ou obtenir la communication des informations personnelles**. Les organismes (toute entité, structure ou personne) habilités à accéder ou à connaître ces informations sont appelés **destinataires, qu'ils soient intérieurs ou extérieurs au mouvement**.

Cela signifie que vous devez **analyser précisément pour chaque traitement mis en place, les responsabilités des différentes entités de votre mouvement** (par exemple : sections locales, unions départementales, fédérations). Celles-ci doivent également respecter les principes énumérés ci-dessous.

À NOTER

Un destinataire est une personne ou un organisme qui reçoit des informations personnelles pour une raison déterminée et légitime. Il doit avoir été autorisé à traiter ces informations. Cela signifie **qu'aucune information personnelle ne doit être divulguée à des personnes n'ayant pas besoin d'en connaître, qu'elles soient internes ou extérieures à l'organisme**.

En pratique

En cas de demande de transmission d'informations personnelles et, plus globalement avant toute communication à des organismes extérieurs, votre organisation syndicale doit s'assurer de la légitimité de cette démarche.

Exemple

L'expert-comptable en charge de la gestion des finances de votre organisation syndicale, les organismes de formation, les entreprises de routage des magazines ainsi que les cabinets de conseils et d'avocats qui vous accompagnent peuvent être destinataires d'informations personnelles.

Vous devez également vous assurer que **cette communication ne porte pas d'atteinte disproportionnée à la vie privée des personnes concernées**. Pour cela, vous devez veiller :

- à ce que les informations soient adéquates, pertinentes et d'un niveau de détail approprié au regard de l'objectif poursuivi par l'éventuel destinataire. Dans certaines circonstances, des informations anonymes pourront par exemple être suffisantes pour le destinataire. *Pour plus d'informations sur la notion d'informations anonymisées, consultez [le glossaire](#) ;*
- à ce que la transmission soit compatible au regard de l'objectif du traitement concerné.

ATTENTION

En pratique, dans la plupart des cas, le responsable des données ne pourra communiquer des informations susceptibles de révéler l'appartenance syndicale de ses adhérents à des destinataires (internes ou extérieurs à votre mouvement) qu'après avoir recueilli l'accord de ces mêmes adhérents.

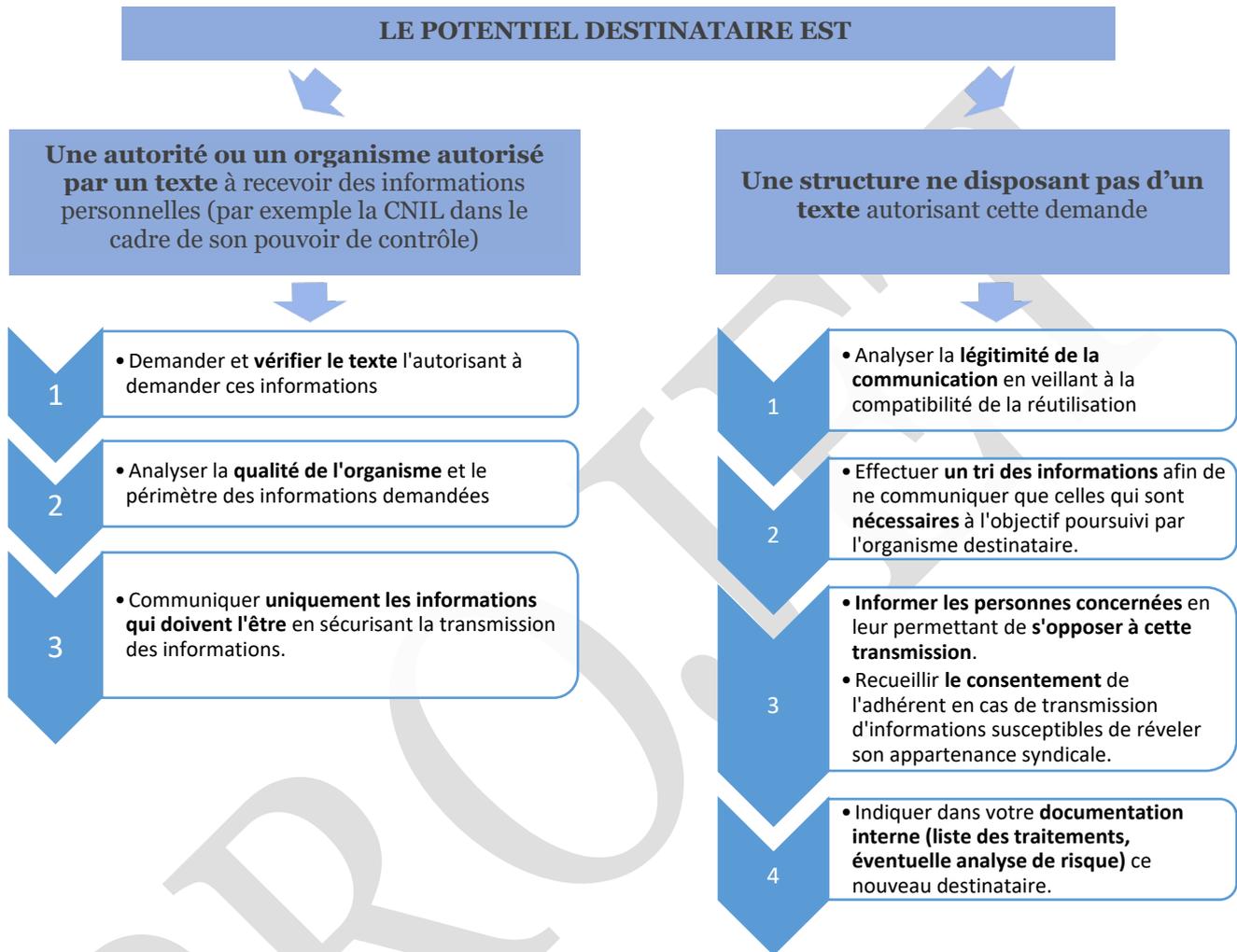
Par exemple, si votre organisation syndicale souhaite organiser un séminaire pour lequel une réservation de chambres d'hôtel est nécessaire, vous devrez alors veiller à ne pas communiquer à cet hôtel des informations susceptibles de révéler l'appartenance syndicale des participants à la formation (par exemple, les adresses emails faisant apparaître l'appartenance syndicale du type : nom.prénom@syndicat.fr) ou à défaut, à demander préalablement l'accord des participants.

À cette fin, une case à cocher peut être prévue directement dans le bulletin d'adhésion pour recueillir leur accord. Celle-ci devra préciser l'objectif de la transmission ainsi que les catégories de destinataires.

Par exemple, vous pouvez insérer la mention suivante :

Je consens à ce que des informations susceptibles de révéler mon appartenance syndicale soient transmises à [organisme(s) destinataire(s)] afin de [raison de la transmission des informations]

Le schéma ci-dessous rappelle le raisonnement à tenir dans une telle situation.



Pour rappel, la liste de l'ensemble des destinataires doit figurer dans la fiche dédiée figurant dans le registre des traitements mis en place par votre organisation syndicale et doit être portée à la connaissance des personnes concernées. *Pour plus d'informations sur le registre des activités de traitement, consultez les [fiches n°8](#) sur l'information des personnes concernées et [n° 10](#) sur les formalités préalables.*

Pour se mettre en conformité :

- vérifier la **légitimité de la demande** de communication d'informations ;
- obtenir l'**accord de la personne concernée** si la demande de communication vise des informations révélant l'appartenance syndicale des personnes concernées ;
- analyser la **pertinence des informations** demandées ainsi que le niveau de détail approprié ;
- préciser les destinataires des informations personnelles dans la **fiche figurant dans la liste des traitements mis en place par votre organisation syndicale** ;
- **informer les personnes concernées** des destinataires ou des catégories de destinataires des informations via la mention d'information.

Références

- [Articles 4, 9 et 32](#) du RGPD sur [cnil.fr](#)
- [Guide tiers autorisés](#) de la CNIL sur [cnil.fr](#)

Fiche n° 7 : Pendant combien de temps votre organisation syndicale peut-elle conserver des informations personnelles ?

Règles de droit

Les informations personnelles ne peuvent pas être conservées indéfiniment : une durée de conservation doit être définie en amont en fonction de l'objectif poursuivi par votre traitement.

Cette durée peut être divisée en deux périodes distinctes :

- la durée de conservation en « **base active** » c'est-à-dire la durée d'exploitation des informations pour l'objectif poursuivi : l'information est **aisément accessible pour la gestion courante de votre organisation syndicale** ;
- la durée de conservation en « **base intermédiaire** » : les informations ne sont plus nécessaires quotidiennement mais **présentent encore un intérêt pour votre organisation syndicale** (gestion d'un éventuel contentieux, réponse à une obligation légale, etc.). Elles ne doivent pouvoir être **consultées que de manière ponctuelle** et par des personnes **spécifiquement habilitées**.

La séparation entre la base active ou la base intermédiaire peut se faire par une solution technique (utilisation d'une autre solution logicielle par exemple) ou *via* la gestion des habilitations.

ATTENTION

L'archivage en base intermédiaire n'est pas systématique. Sa nécessité doit être évaluée au cas par cas. La décision d'archiver certaines informations doit donc répondre à un objectif précis clairement identifié en amont.

Une fois les durées de conservation atteintes, les informations doivent être :

- soit **supprimées**, en veillant à la confidentialité des informations (par exemple en utilisant des poubelles de confidentialité ou en déchiquetant les documents papier avant de les jeter) ;
- soit **anonymisées**, afin que la personne ne soit plus identifiable par qui que ce soit et quel que soit le moyen employé. *Pour plus d'informations sur la notion d'anonymisation, consultez [le glossaire](#).*

ATTENTION

L'anonymisation est une procédure complexe qui suppose que la personne concernée ne soit plus identifiable, par quelque moyen que ce soit, et par toute personne.

Des informations non nominatives qui permettent de reconnaître la personne concernée par recoupement ne sont pas considérées comme étant des informations anonymisées. Elles doivent en conséquence être traitées conformément à la réglementation en vigueur et à l'ensemble des principes présentés dans ce guide.

À NOTER

L'archivage définitif est une phase particulière qui déroge au principe de durée de conservation limitée et permet d'archiver des données sans limitation de durée dans des **conditions très strictes**.

Cette phase concerne **uniquement les traitements mis en œuvre à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques**. *Pour plus d'informations, consultez [le guide sur les durées de conservation](#) disponible sur le site de la CNIL.*

En pratique

Le RGPD fixe un principe mais ne définit pas de durée précise pendant laquelle les informations peuvent ou doivent être conservées. C'est donc à chaque responsable des données de la déterminer au regard de l'objectif du traitement mis en œuvre.

Plusieurs textes peuvent cependant orienter le responsable des données dans la recherche de cette durée de conservation, notamment en ce qui concerne le traitement des informations des salariés de votre organisation syndicale (par exemple, les articles L.3243-4 et D. 3243-8 du code du travail pour les bulletins de paie des salariés).

À défaut de texte, il appartiendra au responsable des données de définir cette durée de manière **proportionnée et cohérente avec l'objectif poursuivi par le traitement**. *Pour plus d'informations, consultez la [fiche n° 1](#) du guide.*

Pour faciliter la recherche de la durée pertinente, la CNIL recommande les durées de conservation suivantes adaptées aux différentes finalités poursuivies par les organisations syndicales.

ATTENTION

Ces durées de conservation ne constituent qu'un point de repère dont vous êtes libres de vous éloigner sous réserve de justifier ce choix dans votre registre des traitements. *Pour plus d'informations, consultez la [fiche n° 10](#) du guide.*

Catégories de traitements	Objectifs du traitement	Exemples d'informations collectées	Durées de conservation conseillées		Justification de la durée de conservation
			Base active	Base intermédiaire	
Gestion administrative	Création de l'association ou de l'organisation syndicale	Les informations personnelles figurant sur la copie de déclaration de l'association en préfecture (ou en mairie pour une organisation syndicale) et les statuts modifiés.	Durée d'existence de l'association ou de l'organisation syndicale	N/A	N/A
	Gestion du fonctionnement de l'organisation syndicale	Les informations personnelles figurant sur les convocations à l'assemblée générale ; les feuilles d'émargement, les pouvoirs ainsi que les procès-verbaux d'assemblée.	1 an	5 ans	N/A
	Gestion fiscale	Les informations personnelles figurant dans les comptes annuels et les pièces justificatives.	1 an	6 ans	art. L.102 du code des procédures fiscales

Catégories de traitements	Objectifs du traitement	Exemples d'informations collectées	Durées de conservation conseillées		Justification de la durée de conservation
			Base active	Base intermédiaire	
Gestion RH	Gestion de la paie	Bulletins de paie	1 mois	5 ans (50 ans en version dématérialisée)	art. L.3243-4 et D. 3243-8 du code du travail
Activités de votre organisation syndicale	Gestion des adhérents et des sympathisants	Nom, prénom, coordonnées	Pendant toute la durée de l'adhésion	3 ans après le dernier contact avec la personne concernée	En cas de perte d'emploi, les adhérents ne renouvellent pas leurs adhésions. Trois ans est la durée estimée d'un retour pérenne à l'emploi et donc d'une éventuelle ré-adhésion à une organisation syndicale.
	Gestion des formations	Nom, prénom, mandat, coordonnées	Jusqu'à ce que la formation ait été entièrement suivie	Certaines informations personnelles pourront être conservées en base intermédiaire pour d'autres besoins (par exemple gestion fiscale et financière). Attention : seules les informations nécessaires doivent être conservées, des informations anonymisées pourront s'avérer suffisantes.	N/A
	Assistance juridique	Toute information personnelle pertinente pour la procédure contentieuse.	Pendant toute la durée de la procédure	Jusqu'à décision définitive ayant autorité de la chose jugée	N/A

Pour se mettre en conformité :

- apprécier **la durée de conservation** envisagée au regard **de l'objectif du traitement** ;
- **documenter sa démarche** afin d'être en mesure de justifier la durée de conservation définie ;
- mettre en place des mesures techniques et organisationnelles pour **supprimer régulièrement** les données à l'expiration des durées de conservation concernées.

Une fois la durée de conservation définie :

- inscrire la durée de conservation au sein du **registre des traitements mis en place par votre organisation syndicale**. *Pour plus d'informations, consultez la [fiche n° 10](#) du guide ;*
- **communiquer les durées de conservation définies** aux personnes concernées à travers les mentions d'information. *Pour plus d'informations, consultez la [fiche n° 8](#) du guide ;*
- **assurer la destruction ou anonymiser les informations** une fois que les durées de conservation fixées ont été atteintes.



Références

- [Article 5 du RGPD](#) sur cnil.fr

Fiche n° 8 : Comment informer les personnes concernées des traitements mis en place ?

Règles de droit

Dans une logique de transparence, le responsable des données (il pourra par exemple s'agir, selon les cas, des **sections syndicales**, des **fédérations** ou des **confédérations**, pour plus d'informations, nous vous invitons à consulter la [fiche n° 2](#) du guide) doit porter à la connaissance des personnes concernées un certain nombre d'éléments lorsqu'il met en place un traitement.

Les informations portées à la connaissance des personnes concernées doivent être **concises, compréhensibles et aisément accessibles** de sorte qu'elles puissent comprendre **la raison précise** de la collecte ou de l'utilisation des informations et **les caractéristiques principales du traitement**.

Cet effort de transparence contribue à la loyauté du traitement mis en œuvre et permet d'instaurer une **relation de confiance** entre votre organisation syndicale et les personnes concernées.

L'information des personnes concernées doit donc intervenir **avant la collecte des informations personnelles**, peu importe la manière dont ces informations ont été collectées, ainsi qu'à chaque **modification importante du traitement** (par exemple l'ajout d'un nouveau destinataire).

Les modalités de l'information seront différentes selon que les informations personnelles auront été **recueillies directement auprès de la personne concernée** (par exemple : remplissage d'un formulaire, réponses apportées aux questions posées lors d'un rendez-vous téléphonique avec la personne concernée, etc.) ou **indirectement**, c'est-à-dire auprès d'un tiers (par exemple : transmission d'une base de données par un autre organisme).

ATTENTION

Lorsque vous obtenez communication d'informations personnelles, vous devez veiller à informer les personnes concernées du traitement que vous souhaitez mettre en place.

Quelles informations doivent-elles être portées à la connaissance des personnes concernées ?

Que les informations personnelles soient collectées auprès des personnes concernées ou auprès de tiers, le responsable des données doit fournir divers éléments.

Dans tous les cas	Selon les caractéristiques du traitement
L'identité et coordonnées de l'organisme, responsable des données.	Lorsque les informations n'ont pas été collectées directement auprès de la personne : les catégories d'informations recueillies et la source de la collecte .
L'objectif poursuivi par le traitement, c'est-à-dire ce à quoi vont servir les informations collectées.	
La base légale ou condition du traitement, c'est-à-dire ce qui autorise le responsable de traitement à traiter des informations personnelles : <ul style="list-style-type: none">• existe-t-il un intérêt légitime pour recueillir les informations personnelles dont l'organisation syndicale a besoin pour l'exercice de ses missions ?• existe-t-il une obligation légale spécifique prévue par un texte ?• la personne concernée a-t-elle donné son accord ?• un contrat (par exemple un contrat d'adhésion ou un contrat de travail) auquel la personne concernée est partie justifie-t-il la mise en place du traitement ?	Si oui, des précisions sur les intérêts légitimes poursuivis par le responsable des données. Si oui, la possibilité de retirer son accord à tout moment.

Dans tous les cas	Selon les caractéristiques du traitement
Le caractère obligatoire ou facultatif du recueil des informations et les éventuelles conséquences pour la personne en cas de non-fourniture.	
Les destinataires ou catégories de destinataires des informations (qui a besoin d'y accéder ou de les recevoir au regard des finalités définies).	
La durée de conservation des informations (ou les critères permettant de la déterminer).	
Les droits des personnes concernées (doivent à minima être mentionnés les droits d'accès, de rectification, d'effacement et le droit à la limitation du traitement)	
Les coordonnées du référent ou du délégué à la protection des données de l'organisme.	
Le droit d'introduire une réclamation auprès de la CNIL.	

En pratique

Comment formuler l'information ?

L'information doit être **aisément compréhensible**. Pour cela, il faut aller à l'essentiel tout en veillant à ce que l'information puisse être comprise par le public visé (par exemple lorsque les personnes concernées peuvent être atteintes de **certaines formes de handicap** rendant pour elles plus difficile la compréhension de l'information ou rendant impossible la lecture d'un support écrit).

Par exemple, le surlignage des informations essentielles figurant dans les mentions d'information présentes sur le site web de votre organisation syndicale peuvent en faciliter la compréhension.

Exemples de mauvaises pratiques :

Les phrases suivantes ne sont pas suffisamment claires pour que l'on comprenne l'objectif du traitement déployé par l'organisation syndicale.

- ◊ « Pour la gestion de votre adhésion, il se peut que nous utilisions vos informations personnelles dans le cadre de procédures » ;
- ◊ « Les informations que nous collectons dans le cadre de votre adhésion sont susceptibles d'être réutilisées pour d'autres raisons ».

Quels supports utiliser pour informer ?

Le support d'information des personnes concernées est libre : **oral, écrit** ou **tout autre moyen**.

Il est ainsi recommandé de prévoir un **double niveau d'information des personnes : collectif et individuel**. Le site web ou l'intranet de l'organisation syndicale peut ainsi intégrer une page dédiée permettant d'informer de façon collective les personnes concernées sur les traitements d'informations mis en place. En complément, une information individuelle devra être effectuée directement auprès des personnes concernées au sein des formulaires d'adhésion, c'est-à-dire avant même la collecte des informations.

Exemples de mauvaises pratiques :

- ◊ Informer les adhérents des traitements de données mis en place **uniquement** au sein des politiques de confidentialité disponibles sur le site web de l'organisation syndicale.
- ◊ Ne pas inclure de mention d'information sur les formulaires d'adhésion au format papier.

En cas de collecte indirecte, l'information doit avoir lieu **dès que possible** (notamment lors du premier contact avec la personne concernée) et, au plus tard dans un délai d'**un mois**.

Exemple de notice d'information à utiliser dans un bulletin d'adhésion dans le cadre d'un double niveau d'information

NB : cet exemple doit être adapté aux spécificités du traitement envisagé.

Les données recueillies à l'occasion de votre adhésion font l'objet d'un traitement par [nom et coordonnées de l'organisation syndicale] lui permettant de gérer votre demande d'adhésion.

À quoi sert le traitement de vos données ?

Le traitement déployé a pour objectif de :

- *traiter votre demande d'adhésion ;*
- *activer votre compte personnel pour accéder aux contenus et services qui vous sont réservés ;*
- *communiquer des informations sur les activités de l'organisation syndicale ;*
- *déterminer le montant de votre cotisation.*

Ce traitement est mis en place dans le cadre du contrat d'adhésion. L'organisation syndicale a également un intérêt légitime informer ses adhérents des activités organisées ainsi que des différentes actualités.

Quels sont vos droits et comment les exercer ?

Vous pouvez accéder aux données vous concernant, les rectifier, demander leur effacement ou exercer votre droit à la limitation du traitement de vos données.

Dans le cadre des traitements relatifs à votre demande d'adhésion, à la détermination de votre cotisation et à l'activation de votre compte personnel pour accéder aux contenus et services qui vous sont réservés, vous disposez également d'un droit à la portabilité de vos données.

Vous disposez également du droit de vous opposer aux traitements mis en œuvre dans le cadre de la communication des informations sur les activités de l'organisation syndicale.

Pour toute question relative à la protection de vos données ou pour exercer vos droits, vous pouvez contacter le délégué à la protection des données de [identité de l'organisation syndicale à mentionner] à l'adresse suivante : [courriel du DPO ou adresse postale à renseigner].

Pour en savoir plus sur les traitements d'informations mis en œuvre nous vous invitons à consulter notre politique de confidentialité disponible à l'adresse suivante : [adresse de la politique de confidentialité du site web de l'organisation syndicale]

Si vous estimez, après avoir contacté [nom de l'organisation syndicale], que vos droits « informatique et libertés » ne sont pas respectés, vous pouvez adresser une réclamation en ligne à la CNIL.

Pour se mettre en conformité :

- construire des **supports d'information compréhensibles et adaptés au public visé** ;
- mettre **en exergue les informations essentielles** ;
- informer individuellement les personnes concernées en utilisant, si possible, **un double niveau d'information** ;
- s'il existe un référent ou délégué à la protection des données, **travailler de concert avec celui-ci** sur le moyen envisagé pour informer les personnes concernées.

Références

- [Articles 12, 13 et 14](#) du RGPD sur cnil.fr
- [Lignes directrices du CEPD du 11 avril 2018 sur la transparence](#) sur cnil.fr

Fiche n° 9 : Quelles mesures votre organisation syndicale doit-elle prendre pour garantir les droits des personnes concernées ?

Règles de droit

Quelles que soient les caractéristiques du traitement, les personnes concernées disposent de plusieurs droits leur permettant de garder la maîtrise de leurs informations personnelles.

Il vous appartient de leur expliquer comment exercer les différents droits :

Droit d'accès



Le droit d'accès permet à une personne concernée d'obtenir :

- la confirmation que votre organisation syndicale détient des informations personnelles la concernant afin d'en vérifier l'exactitude ;
- la copie de ses informations personnelles ;
- des éléments expliquant le traitement mis en œuvre par l'organisation syndicale (par exemple : objectifs, destinataires, durée de conservation, etc.).

Droit de rectification



Une personne concernée peut demander que ses informations personnelles soient rectifiées si elles sont inexactes ou incomplètes. Cela permet à l'organisation syndicale de ne pas utiliser ou diffuser des informations erronées.

Par exemple, en cas de déménagement, un adhérent peut demander à ce que son adresse postale soit modifiée.

Droit d'effacement



Une personne concernée est en mesure d'exiger l'effacement de ses informations si :

- les informations ne sont plus nécessaires à votre organisation syndicale au regard de l'objectif poursuivi ;
- les informations ont fait l'objet d'un traitement non autorisé ;
- les informations doivent être effacées pour respecter une obligation légale ;
- la personne concernée a retiré son accord pour traiter ses informations personnelles.

Droit à la limitation ou « gel » des données

Une personne concernée peut demander à « geler » l'utilisation de ses informations personnelles dans deux situations :



- si elle conteste l'exactitude des informations, le temps que votre organisation syndicale effectue une vérification ;
- si votre organisation syndicale souhaite supprimer les informations mais que la personne concernée souhaite quant à elle les conserver, notamment pour exercer un autre droit (par exemple en cas de contentieux, le temps que la personne concernée obtienne la copie de ces informations).

En plus de ces droits, une personne concernée pourra disposer de droits complémentaires en fonction de la condition/base légale du traitement. *Pour plus d'informations sur l'identification des bases légales nous vous invitons à consulter la [fiche n° 3](#) du guide.*

Droit d'opposition



Pour les traitements fondés sur l'intérêt légitime, la personne concernée a le droit de s'y opposer pour des raisons tenant à sa situation particulière.

Votre organisation syndicale doit alors cesser de traiter ses informations personnelles sauf si vous êtes en mesure de justifier de l'existence de motifs légitimes et impérieux prévalant sur les intérêts de la personne concernée.

Droit à la portabilité



Une personne concernée peut demander la portabilité de ses informations personnelles, c'est-à-dire soit les récupérer soit demander à les transférer vers un organisme de son choix, sous réserve que :

- les informations personnelles fassent l'objet d'un traitement automatisé ;
- le traitement soit fondé sur la condition/base légale de l'accord de la personne concernée ou sur l'exécution d'un contrat.

Les conditions d'exercices de ces différents droits sont récapitulées dans le tableau ci-après. Les cases ✓ indiquent que l'exercice du droit est possible.

À NOTER

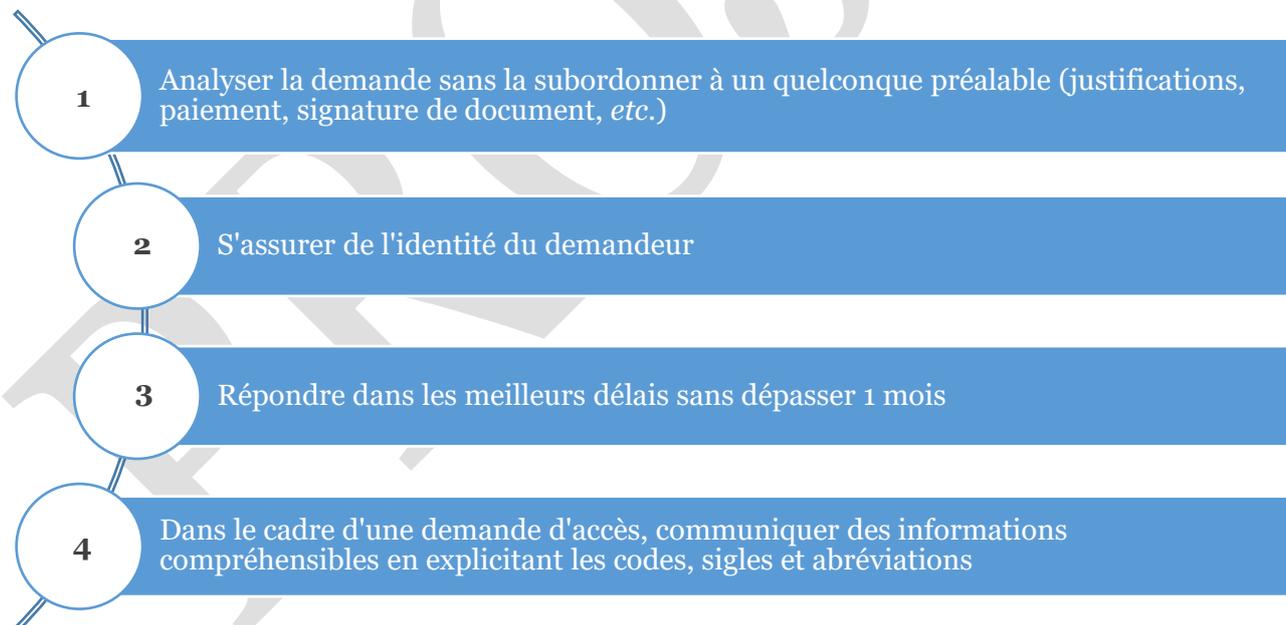
L'ensemble de ces droits s'appliquent aux informations collectées directement auprès de la personne concernée et à celles obtenues auprès d'organismes tiers. Par exemple, si votre organisation syndicale achète un fichier, elle doit permettre aux personnes concernées d'exercer leurs droits, même si vous n'êtes pas à l'origine de la collecte de ces informations.

Par ailleurs, l'exercice de ces droits ne doit **pas porter atteinte aux droits des tiers**. Par exemple, cela signifie que seules les informations relatives à la personne concernée peuvent lui être communiquées dans le cadre de l'exercice du droit d'accès.

Droits de la personne	Accès	Rectification	Opposition	Effacement	Limitation/ Gel des données	Portabilité
Recueil de l'accord de la personne concernée	✓	✓	✗	✓	✓	✓
Exécution du contrat	✓	✓	✗	✓	✓	✓
Respect d'une obligation légale	✓	✓	✗	✓	✓	✗
Intérêt légitime	✓	✓	✓	✓	✓	✗

En pratique

Lorsqu'elle reçoit une demande d'exercice d'un droit, votre organisation syndicale doit procéder en quatre étapes :



Afin de pouvoir être en mesure de répondre à ces demandes dans les délais prévus, une procédure peut être définie en collaboration avec le délégué à la protection des données afin de :

- définir les rôles de chacun pour être en mesure de répondre facilement ;
- encadrer les différentes étapes de gestion de la demande.

À NOTER

Dans de rares cas, des frais raisonnables liés à une demande particulière (par exemple, demande d'une copie supplémentaire) pourront être demandés.

Si la demande est complexe à traiter ou si votre organisation syndicale doit faire face à de nombreuses demandes, vous pouvez porter le délai de réponse à **trois mois**, sous réserve d'en avoir informé la personne concernée au terme du délai initial d'un mois.

ATTENTION

S'agissant de la vérification de l'identité du demandeur, votre organisation syndicale ne doit pas automatiquement demander une pièce d'identité : par exemple, lorsqu'un adhérent effectue la demande à travers son espace adhérent en ligne supposant une identification, il n'apparaît pas nécessaire de demander un justificatif d'identité.

Quelques exemples de bonnes pratiques pour le traitement des demandes :

- Vous pouvez prévoir un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée pour l'exercice des droits des personnes concernées.
- Si vous disposez d'un site web proposant la création d'un compte utilisateur aux adhérents, il est recommandé de donner la possibilité d'exercer les droits à partir de cet espace personnel.

Pour se mettre en conformité :

- **identifier la condition/base légale** des traitements mis en place pour déterminer les droits susceptibles de pouvoir être exercés par les personnes concernées ;
- **informer les personnes concernées**, pour plus d'informations, nous vous invitons à consulter [la fiche n° 8](#) du guide ;
- **explicitier** toute information susceptible de ne pas être comprise par la personne concernée (par exemple, les sigles) ;
- **encadrer les rôles et les étapes en interne** pour être en mesure de répondre aux demandes d'exercice des droits dans le temps imparti.

📖 Références

- [Articles 15, 16, 17, 18](#) et [21](#) du RGPD

Fiche n° 10 : Une organisation syndicale doit-elle effectuer des formalités avant de mettre en place un traitement ?

Règles de droit

Dans la continuité des anciennes règles prévoyant une dispense de déclaration pour les traitements mis en œuvre par les organisations syndicales, le RGPD établit une logique de responsabilisation des acteurs pour tous les organismes.

Votre organisation doit donc adopter **une démarche continue de conformité** à travers l'élaboration d'une documentation et de procédures permettant de démontrer le respect des règles relatives à la protection des données.

Pour cela, elle doit notamment :

- tenir un registre des traitements mis en place ;
- mener des analyses d'impact relatives à la protection des données (« AIPD ») pour les traitements présentant « **un risque élevé** » pour les personnes ;
- assurer une **information complète et adaptée des personnes concernées** sur les traitements mis en place. *Pour plus d'informations, nous vous invitons à consulter la [fiche n° 8](#) du guide ;*
- formaliser **les rôles et responsabilités des différents acteurs** qui interviennent dans les traitements mis en place (ex. : contrat de sous-traitance passé) ;
- documenter **les mesures prises pour garantir la sécurité** des informations personnelles ;
- désigner un référent ou un **délégué à la protection des données** (DPD ou DPO pour *Data Protection Officer*).

En pratique

Le registre des traitements mise en place par votre organisation syndicale (liste détaillée des traitements d'informations personnelles) : à quoi sert cet outil et comment le mettre en place ?

Ce registre est un outil de pilotage qui participe à la documentation de la conformité. Grâce à ce document, votre organisation syndicale peut recenser et analyser tous les traitements d'informations personnelles qu'elle met en œuvre.

Cette cartographie des traitements doit lui permettre de déterminer précisément :

- les **parties prenantes** (notamment les sous-traitants et responsable(s) des données) qui interviennent dans le traitement des informations personnelles collectées ;
- les **catégories d'informations personnelles** collectées ;
- **à quoi servent** les informations collectées (ce que l'organisation syndicale en fait), **qui peut y accéder** et **à qui elles sont communiquées** ;
- **combien de temps les informations personnelles sont conservées** ;
- si des **transferts d'informations vers des pays tiers** sont prévus et dans ce cas, les garanties associées à ces transferts ;
- comment ces informations sont **sécurisées**.

ATTENTION

Le responsable des données doit veiller à **justifier ses choix**, c'est-à-dire qu'il doit **démontrer en quoi les caractéristiques du traitement sont appropriées à ses besoins**.

Afin d'avoir une documentation complète, **divers documents doivent être annexés au registre** : audit de sécurité, contrat de sous-traitance, etc.

Le registre des traitements doit se présenter sous une forme écrite, qui peut être au format papier ou électronique. Chaque fiche qui le compose présente les caractéristiques d'un traitement et doit être modifiée dès lors qu'une transformation est opérée sur le traitement (nouvelles informations collectées, allongement de la durée de conservation, etc.).

Cet outil **est un document interne que vous devez conserver**. Il ne doit pas être envoyé à la CNIL, sauf si elle le demande.

Exemple : page d'un registre de traitements d'un syndicat dédiée à l'activité de gestion des adhésions

L'exemple ci-dessous (sur deux pages) concerne le traitement qui serait mis en place par une organisation syndicale pour recevoir, analyser et traiter des demandes d'adhésions.

Registre des activités de traitements mis en place par [identité du responsable des données à compléter] Activité : Gestion des adhésions	
Responsable des données	[Identité du responsable des données à renseigner]
Coordonnées du délégué à la protection des données (DPO)	[Coordonnées du DPO à renseigner]
Objectifs du traitement	Gestion des adhérents
Objectif n° 1	Traitement des demandes d'adhésion
Objectif n° 2	Détermination du montant de la cotisation
Base légale du traitement	Exécution du contrat d'adhésion <i>Pour plus d'informations, nous vous invitons à consulter la fiche n° 3.</i>
Catégories des personnes concernées	Personnes ayant présenté une demande d'adhésion
Catégories des informations personnelles traitées	<ul style="list-style-type: none"> • Informations relatives à l'identité et aux coordonnées • Informations relatives à l'activité professionnelle, la catégorie socio-professionnelle • Informations relatives à la rémunération • [À compléter par le responsable des données]
Source des informations	Informations fournies directement par la personne concernée
Caractère obligatoire ou facultatif du recueil des informations et conséquences en cas de non-fourniture	La fourniture des informations par la personne concernée est obligatoire pour la gestion de l'adhésion répondant aux objectifs susvisés
Catégories de destinataires des informations	En fonction de leurs besoins respectifs, sont destinataires de tout ou partie des informations : [à indiquer par le responsable des données] <p style="text-align: center;">ATTENTION</p> Seul l'accord de la personne concernée autorise le responsable des données à communiquer des informations relatives à son appartenance syndicale.

Registre des activités de traitements mis en place par [identité du responsable des données à compléter]

Activité : Gestion des adhésions

Transfert des informations vers un pays tiers de l'Union européenne ou vers une organisation internationale	Le traitement ne prévoit pas de transfert des informations hors de l'Union européenne.
Prise de décision automatisée	Le traitement ne prévoit pas de prise de décision automatisée.
Durée de conservation des informations	Le temps de l'adhésion puis 3 ans après le dernier contact avec la personne concernée. <i>Pour plus d'informations, nous vous invitons à consulter la fiche n° 7 du guide.</i>
Mesures de sécurité techniques /organisationnelles (description générale)	<input type="checkbox"/> Contrôle d'accès des utilisateurs (décrivez les mesures) : <input type="checkbox"/> Mesures de traçabilité (décrivez les mesures) : <input type="checkbox"/> Mesures de protection des logiciels (décrivez les mesures) : <input type="checkbox"/> Sauvegarde des données (décrivez les mesures) : <input type="checkbox"/> Contrôle des sous-traitants (décrivez les mesures) : <input type="checkbox"/> Autres mesures : [À renseigner par le responsable des données] <i>Pour plus d'informations, consulter la fiche n° 1 relative aux mesures de sécurité.</i>
Droits des personnes concernées	Les personnes concernées disposent : <ul style="list-style-type: none"> • des droits qui s'appliquent pour tous les traitements d'informations personnelles : les droits d'accès, de rectification et droit à l'effacement de leurs informations personnelles ainsi que le droit à la limitation du traitement ; • d'un droit découlant du choix de la base légale de l'exécution du contrat : le droit à la portabilité des données. Pour toute information ou aide dans l'exercice des droits, contacter le délégué à la protection des données
Droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL)	<ul style="list-style-type: none"> • Pour contacter la CNIL: https://www.cnil.fr/fr/vous-souhaitez-contacter-la-cnil • Pour adresser une réclamation auprès de la CNIL: https://www.cnil.fr/fr/plaintes
Rédacteur (s) de la fiche	[Fonction du (des) rédacteur(s) à renseigner]
Date des mises à jour	[Date des mises à jour à renseigner]

Quand votre organisation syndicale doit-elle mener une analyse d'impact relative à la protection des données « AIPD » ?

Votre organisation syndicale doit réaliser une analyse d'impact dès lors que le traitement qu'elle met en œuvre est susceptible de présenter un risque élevé pour les droits et les libertés des personnes concernées.

La réalisation d'une analyse d'impact est obligatoire dès lors **qu'au moins deux critères sont remplis parmi les neuf critères suivants** :

- évaluation ou notation d'une personne ;
- prise de décision automatisée ;
- surveillance systématique ;
- traitement d'informations sensibles ou à caractère hautement personnel (notamment l'appartenance syndicale) ;
- traitement à grande échelle ;
- croisement ou combinaison d'ensembles d'informations personnelles ;
- informations concernant des personnes vulnérables ;
- utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
- traitements qui empêchent les personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Par exemple, le traitement relatif à la gestion de votre fichier d'adhérents pourrait devoir faire l'objet d'une analyse d'impact car il contient des **informations sensibles** (appartenance syndicale) potentiellement traitées à **grande échelle** (grand nombre de personnes concernées et volume important d'informations personnelles).

ATTENTION

Votre organisation syndicale doit mener une analyse d'impact **avant la mise en place** du traitement. Elle doit donc être démarrée le plus en amont possible et devra être mise à jour tout au long du cycle de vie du traitement.

L'analyse d'impact se décompose en trois parties :

- une **description détaillée du traitement** mis en place, comprenant tant les aspects techniques qu'opérationnels ;
- une **évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux** (objectif, informations personnelles et durées de conservation, information et droits des personnes, etc.), qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;
- une **évaluation des risques sur la sécurité des informations** (confidentialité, intégrité et disponibilité) ainsi que leur impact potentiel sur les personnes concernées s'ils se matérialisent, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les informations personnelles.

Le référent ou le DPO (si votre organisation syndicale en a désigné un) devra être consulté. Dans le cas où l'analyse d'impact indique qu'elle ne parvient pas à identifier des mesures suffisantes pour réduire les risques élevés à un niveau acceptable, vous devez consulter la CNIL préalablement à la mise en place du traitement.

Pour se mettre en conformité :

- **se poser les bonnes questions en amont du traitement** : avez-vous vraiment besoin de certaines informations concernant l'adhérent dans le cadre de votre traitement ? Est-il pertinent de conserver les informations aussi longtemps ? Les informations sont-elles suffisamment protégées ? etc. ;
- veiller à **renseigner et à mettre à jour régulièrement la fiche dédiée dans le registre des traitements mis en place par votre organisation syndicale** ;

- **vérifier en fonction des caractéristiques du traitement, si une analyse d'impact doit être réalisée** et, pour ce faire, apprécier dans quelle mesure le traitement envisagé présente un risque élevé pour les personnes concernées.

La CNIL propose des outils méthodologiques ainsi que des modèles pour accompagner les responsables des données dans la réalisation d'une analyse d'impact et la constitution du registre des traitements mis en place. Votre organisation syndicale peut les consulter sur le site web de la CNIL.

Références

- [Articles 30 et 35](#) du RGPD sur [cnil.fr](#)
- [L'analyse d'impact relative à la protection des données \(AIPD\)](#) sur [cnil.fr](#)
- [Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données \(AIPD\)](#) sur [cnil.fr](#)
- [Lignes directrices du 4 avril 2017 du CEPD concernant l'analyse relative à la protection des données et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé](#) sur [cnil.fr](#)
- [Guide sur la sécurité des données personnelles de la CNIL \(édition 2018\)](#) sur [cnil.fr](#)

Fiche n° 11 : Comment sécuriser les informations personnelles traitées et ne les communiquer qu'aux personnes autorisées ?

Règles de droit

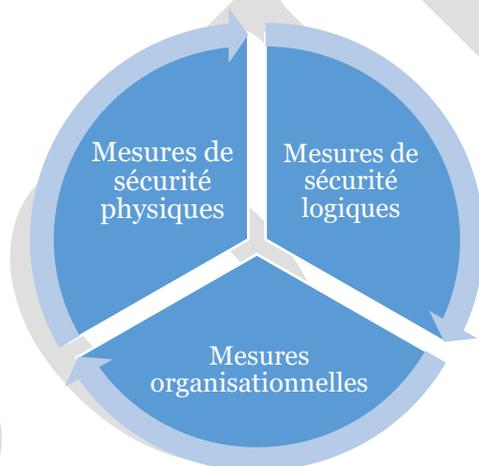
Votre organisation syndicale doit assurer la sécurité et la confidentialité des informations personnelles qu'elle traite. Pour cela, elle doit veiller à ce que seules les personnes ayant besoin d'en connaître en raison de leurs fonctions puissent y accéder et doit également limiter la liste des personnes à qui les informations sont susceptibles d'être communiquées. *Pour plus d'informations, consultez la [fiche n° 6](#) relative aux organismes habilités à accéder à des informations personnelles.*

Parallèlement, elle doit mettre en place des mesures afin de limiter le risque d'atteinte à la confidentialité, la disponibilité et l'intégrité des informations personnelles qu'elle traite.

Ces mesures de sécurité doivent être adaptées au niveau du risque encouru par les personnes dont vous détenez les données, qui peut être d'autant plus important que votre organisation traite des informations sensibles telles que l'appartenance syndicale.

En pratique

Pour assurer la sécurité des informations personnelles traitées, diverses précautions élémentaires peuvent être prises. Plusieurs types de mesures complémentaires doivent être mises en place :



1- Mesures de sécurité physiques

Votre organisation syndicale doit définir et mettre en œuvre des mesures physiques (ex : verrouillage des portes et des armoires) afin de **sécuriser l'accès aux locaux**, et plus particulièrement aux salles hébergeant les serveurs informatiques et les différents éléments du réseau. Les documents papier contenant des données personnelles doivent également faire l'objet de mesures de sécurité physiques.

À NOTER

Votre organisation syndicale peut par exemple installer des alarmes anti-intrusion et vérifier régulièrement leur bon fonctionnement, installer des serrures dans chaque bureau et veiller à leur fermeture lors des absences du personnel, et stocker les documents papier dans des armoires verrouillées.

2- Mesures de sécurité logiques

Il est également nécessaire de définir **et de mettre en œuvre des mesures logiques** :

Sécurisation du poste de travail

- Il est par exemple recommandé de paramétrer les postes de travail pour qu'ils se **verrouillent automatiquement** à l'issue d'une courte période d'inactivité de l'utilisateur.
- Il est également recommandé de **chiffrer les postes de travail**, et de réaliser des sauvegardes régulières des données.

Traçabilité

- **Responsabiliser l'ensemble des acteurs** en les informant de la mise en place d'une procédure de traçabilité des actions sur les fichiers ;
- **Procéder au contrôle régulier des traces** en utilisant des procédés de détection automatisés d'actions suspectes.

Mots de passe

Adopter **une politique rigoureuse de mot de passe pour l'accès aux postes de travail et à certains fichiers** (utilisation de mot de passe unique, nécessité de définir des mots de passe robustes, etc.). Vous pouvez vous référer aux recommandations de la CNIL en la matière.

À NOTER

Les recommandations de la CNIL en termes de taille et de complexité du mot de passe varient en fonction des mesures complémentaires mises en place. Ainsi, si une authentification est basée exclusivement sur un mot de passe, il est nécessaire que celui-ci remplisse *a minima* les critères suivants :

- ⊗ au moins 12 caractères ;
- ⊗ des majuscules et des minuscules ;
- ⊗ des chiffres et caractères spéciaux.

Pour protéger le réseau informatique interne et les serveurs des attaques extérieures, vous êtes par ailleurs invité à mettre en place des dispositifs tels que des **pare-feu** et **antivirus** régulièrement mis à jour et à utiliser des **canaux sécurisés** et des **systèmes d'authentification** pour les connexions à distance et en **chiffrant systématiquement les informations** stockées sur des supports nomades tels que les ordinateurs portables, les smartphones et les clefs USB.

3- Mesures de sécurité organisationnelles

Pour garantir un niveau de sécurité suffisant, **les mesures logiques ou physiques doivent être couplées à des mesures organisationnelles.**

La sécurité organisationnelle regroupe toutes les procédures qui permettent de **structurer l'application des mesures de sécurité précitées et d'assurer leur effectivité.** Elles permettent à votre organisation syndicale de :



Votre organisation syndicale peut ainsi choisir de diffuser et faire signer à chaque utilisateur une **charte informatique** rappelant les conditions d'utilisation des équipements informatiques et des informations personnelles et de sensibiliser régulièrement les utilisateurs aux règles et aux menaces existantes.

À NOTER

Lorsque votre organisation syndicale a recours à des prestataires extérieurs, vous devez vous assurer d'encadrer contractuellement vos exigences en matière de sécurité. Votre responsabilité peut le cas échéant être engagée.

Pour se mettre en conformité :

- établir une **charte informatique** rappelant les obligations de chacun ;
- prendre connaissance du [guide sur la sécurité des données de la CNIL](#) qui permettra de vous accompagner dans la définition des mesures de sécurité nécessaires ainsi que des **recommandations de l'Agence nationale de sécurité des systèmes d'information (ANSSI)**, par exemple [celles relatives à la sécurisation des sites web](#) ;
- lorsque votre traitement est susceptible de présenter des risques élevés pour les droits et libertés des personnes concernées, vous devez réaliser **une analyse d'impact relative à la protection des données (AIPD)** pour gérer ces risques et mettre en place les mesures adaptées permettant de les limiter à un niveau acceptable (*Pour plus d'informations, nous consultez la [fiche n° 10](#) relative aux formalités préalables*).

Références

- [Article 32 à 35](#) du RGPD sur [cnil.fr](#)

Fiche n° 12 : Quelles précautions prendre lors du choix des outils de votre organisation syndicale ?

Règles de droit

Votre organisation syndicale est responsable des données lorsqu'elle traite des informations personnelles à partir d'un outil qu'elle a elle-même choisi. Quel que soit l'outil utilisé par votre organisation syndicale, toutes les règles existantes en matière de protection des informations personnelles doivent être respectées : les outils les plus respectueux de la vie privée des personnes concernées devront donc être privilégiés.

En effet, le choix de l'outil peut avoir des **conséquences importantes pour les informations personnelles des personnes concernées**. Un outil peut par exemple :

- procéder à la collecte, plus ou moins légalement, d'un nombre important d'informations sans aucun lien avec l'objectif du traitement (ainsi, par exemple, la copie de tous les contacts enregistrés dans le carnet d'adresses d'un téléphone mobile) ;
- intégrer des « pisteurs publicitaires » pouvant par exemple collecter à l'insu des utilisateurs des informations d'utilisation du terminal mobile (la géolocalisation, la liste des applications installées, les comptes associés au terminal...), etc. ;
- compromettre la sécurité du matériel informatique des personnes concernées ;
- transférer des informations personnelles vers des pays en dehors de l'Union européenne pour des raisons tenant à l'administration de l'hébergement ou au respect des lois des pays auxquels l'entité-mère ou l'entreprise est soumise.

En pratique

Afin d'assurer la protection des informations personnelles des personnes concernées, il est important que votre organisation syndicale puisse mener une réflexion sur le choix des outils avant d'y avoir recours.

Trois conseils peuvent guider cette démarche « au cas par cas » :

- privilégier les outils faisant **preuve de transparence** dans leur fonctionnement ;
- préférer les outils **qui collectent un minimum d'informations** et les plus respectueuses des droits des personnes concernées ;
- vous assurer que l'outil **ne procède pas à des transferts d'informations personnelles** vers des pays tiers qui ne seraient pas encadrés juridiquement **en choisissant un hébergement à même de garantir l'absence de tout transfert d'informations** vers des pays dont la législation ne serait pas compatible avec le droit européen ou en **mettant en place des mesures à même de garantir un niveau de protection adéquat** des informations personnelles.

Cette **démarche devra être documentée** et pourra être formalisée, le cas échéant, dans le cadre d'une analyse d'impact relative à la protection des données (*Pour plus d'informations, nous vous invitons à consulter la [fiche n° 10](#) sur les formalités préalables*).

Pour se mettre en conformité :

- évaluer le **besoin** du recours à ces outils ;
- **s'informer de la manière dont les informations sont traitées par le fournisseur de l'outil en veillant à ce que les règles relatives à la protection des données soient respectées ;**
- **vérifier la présence de transfert d'informations personnelles vers des pays tiers** et, si c'est le cas, se référer aux articles 44 et suivants du RGPD ;
- **privilégier les outils minimisant le volume des informations collectées ;**
- **informer** les personnes concernées préalablement à la mise en place de ces outils ;
- si votre organisation syndicale en a désigné un, associer le **référént ou le délégué à la protection des données** à la démarche de mise en conformité.

Références

- [Articles 5, 6 et 24](#) et suivants du RGPD sur [cnil.fr](#)
- [Transférer des données hors de l'UE](#) sur [cnil.fr](#)

Glossaire

	Définition	Fiches associées
Analyse de risques ou (analyse d'impact sur la vie privée)	Outil permettant d'analyser les risques d'un projet de traitement pour les droits et libertés des personnes dont les données sont traitées, afin de les limiter pour construire un traitement respectueux de la vie privée.	10
Anonymisation	Technique permettant de rendre impossible l'identification de la personne concernée, qu'importe le moyen employé.	7
Archivage intermédiaire ou base intermédiaire	Base de données dont l'accès est particulièrement circonscrit car les informations ne sont pas nécessaires pour la gestion courante mais dont la conservation est importante pour l'organisme, pour se prémunir d'un éventuel contentieux par exemple.	7
Base active	Base de données permettant l'usage courant des informations personnelles c'est-à-dire l'exploitation courante des informations qui sont en conséquence aisément accessible.	7
Habilitation	Droits octroyés à des personnes pour accéder et/ou modifier les informations dans un document, une base de données, <i>etc.</i>	6 et 11
Pseudonymisation	Technique permettant de ne plus identifier directement la personne concernée. Il est cependant possible de retrouver son identité.	1