**Entreprises**
Publié le 19/11/2022 – Mis à jour le 01/02/2023

**Obligations en matière de protection des données personnelles (RGPD)**
Toute entreprise qui réalise un traitement de données (gestion de la paie, recrutement, fichier clients ou fournisseurs…) doit respecter le **Règlement général sur la protection des données (RGPD)**. Il s'applique à **toute entreprise**, **quelle que soit sa taille et son secteur d'activité**, dès lors qu'elle est établie sur le territoire de l'Union européenne ou que son activité cible directement des résidents européens.

**Traitement de données personnelles : définition**

Il est nécessaire de définir la notion de **donnée personnelle** pour comprendre ce que recouvre le **traitement de données personnelles**.

**Qu'est-ce qu'une donnée personnelle ?**
Une donnée personnelle ou « donnée à caractère personnel » est une **information se rapportant à une personne physique identifiée ou identifiable** (ex : nom, prénom, numéro de sécurité sociale, adresse, numéro de téléphone, adresse mail, photo, empreinte, donnée de géolocalisation, adresse IP ou identifiant en ligne).
Une personne est dite **identifiée** lorsque l'on connaît son identité. Une personne est **identifiable** lorsqu'elle peut être identifiée, quand bien même ses nom et prénom resteraient inconnus, à partir du **croisement d'un ensemble de données** (ex : une femme vivant à telle adresse, née tel jour et membre de telle association).

**À noter**
Peu importe que l'information soit **publique ou confidentielle** et **peu importe le support** sur lequel se trouve l'information (formulaire papier, clé USB, disque dur, caméra, etc.).
En revanche, une donnée n'est plus personnelle lorsqu'elle est **anonymisée**, éliminant ainsi toute possibilité d'identifier la personne concernée.
De même, une donnée n'est pas personnelle lorsqu'elle se rapporte à une **personne morale** (ex : une entreprise, une association).

**Exemple**
L'adresse postale, le numéro de téléphone du standard ou une adresse mail générique (ex : « compagnie1[@]email.fr ») d'une entreprise ne sont pas des données personnelles.

**Qu'est-ce qu'un traitement de données personnelles ?**
Un traitement de données personnelles consiste en **toute opération portant sur des données personnelles**, quel que soit le procédé utilisé (ex : la collecte, l'enregistrement, la conservation, la modification, la consultation, la diffusion ou l'effacement de données).
Autrement dit, on parle de traitement de données dès que les données d'une personne sont utilisées d'une manière ou d'une autre et peu importe à qui appartiennent ces données (un **client**, un **fournisseur**, un **prestataire**, un **employé**, un **candidat à l'embauche**, etc.).
Un traitement de données personnelles n'est pas nécessairement informatisé, **les fichiers papier sont également concernés** et doivent être protégés dans les mêmes conditions.

**Exemple**
Création d'un fichier clients ou fournisseurs (papier ou informatisé)
Consultation d'un tableau Excel contenant des données de ressources humaines (bulletins de paie, contrats de travail, CV et lettres de motivation…)
Prospection commerciale par courrier ou par e-mail
Livraison d'une commande
Conservation d'adresses IP
Enregistrement de vidéosurveillance dans un magasin
Destruction de documents papiers contenant des données personnelles.

**À savoir**
D'une manière générale, **dès qu'une entreprise emploie du personnel**, les services des ressources humaines sont amenés à effectuer un traitement de données des employés (gestion de la paie, recrutement, contrats de travail…) et sont donc **systématiquement concernés par le RGPD**.
Pour être conforme au RGPD, le traitement de données doit obéir aux **principes suivants** :

Le traitement doit être **licite** : il doit être fondé sur l'une des 6 bases légales fixées par le RGPD notamment le consentement de la personne concernée, l'exécution d'un contrat ou le respect d'une obligation légale.
Le traitement doit être **transparent** : la personne dont les données sont collectées doit être informée de la collecte et de sa finalité, ainsi que des droits dont elle dispose sur ses données (accès, rectification, portabilité, effacement…).
Le traitement doit avoir une **finalité** : le responsable du traitement doit définir l'objectif poursuivi par la collecte des données (ex : prospection, suivi de relations clients, ressources humaines). Les données ne doivent pas être traitées d'une manière incompatible avec cette finalité.
Le traitement doit être **proportionnel et pertinent** : seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées. On parle de « principe de minimisation ». Par exemple, une société n'a pas à collecter le numéro de téléphone de ses clients lorsqu'elle adresse uniquement de la prospection par mail.
Le traitement doit être **temporaire** : la durée de conservation des informations doit être définie dès la mise en place du dispositif qui collecte ces données. Une fois l'objectif atteint, les informations collectées ne sont plus nécessaires et doivent donc être supprimées.
Le traitement doit être **sécurisé** : toutes les mesures nécessaires pour garantir la sécurité, et notamment la confidentialité des données personnelles doivent être mises en place (ex : mots de passe, https, sauvegarde). Ces mesures de sécurité sont proportionnelles aux risques encourus (ex : vol ou perte de données).
Sauf exceptions, tout traitement portant sur des données dites **sensibles** est **interdit**. Il s'agit d'une **catégorie de données éminemment personnelles** qui sont susceptibles de conduire à des discriminations si elles sont révélées (ex : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, orientation sexuelle, appartenance syndicale, données génétiques).

**Qui est responsable du traitement ?**

Le représentant légal de l'entreprise (chef d'entreprise, gérant, président…) est désigné «**responsable du traitement** ». Le responsable du traitement est la personne **à l'initiative du traitement de données**, il détermine ses finalités et ses moyens.
Le plus souvent, le responsable de traitement a recours à un **sous-traitant** chargé de traiter les données pour le compte du responsable du traitement (ex : hébergement de données, maintenance informatique, service d'envoi de messages de prospection commerciale).
Le responsable du traitement et son sous-traitant doivent respecter de **nombreuses obligations** en matière de protection des données personnelles.

## Informer les personnes concernées

Le responsable du traitement doit **informer toute personne** dont les données sont collectées.
Cette obligation s'applique que la collecte soit **directe** (ex : données recueillies auprès de la personne dans un formulaire) ou **indirecte** (ex : données récupérées auprès de partenaires commerciaux, de data brokers ou de sources accessibles au public).
L'information doit être délivrée **au moment de la collecte** (en cas de collecte directe) ou dans un délai raisonnable après avoir obtenu les données, sans dépasser **1 mois** (en cas de collecte indirecte).

**Quelles informations faut-il délivrer ?**

Le responsable du traitement doit transmettre les **informations suivantes** :
Identité et coordonnées du responsable du traitement
Coordonnées du délégué à la protection des données (DPO), le cas échéant
Finalité poursuivie par le traitement : c'est-à-dire à quoi vont servir les données personnelles collectées
Base légale justifiant le traitement : il peut s'agir du consentement de la personne, du respect d'une obligation prévue par un texte de loi, de l'exécution d'un contrat, etc.
Caractère obligatoire ou facultatif de la fourniture de données personnelles : les conséquences pour la personne en cas de non-fourniture des données
Destinataires des données personnelles : qui va recevoir et accéder aux données (service interne compétent, prestataire, etc.)
Durée de conservation des données personnelles
Droits de la personne sur ses données : droit de refuser la collecte, droit d'accéder, de rectifier et d'effacer ses données
Droit de la personne d'introduire une réclamation auprès de la Cnil
Source d'où proviennent les données personnelles, en cas de collecte indirecte
Existence d'un transfert des données personnelles vers un pays hors de lUnion européenne, le cas échéant.

**Comment délivrer l'information ?**

Les informations doivent être transmises de façon **concise, transparente, compréhensible et facilement accessible**, en des termes clairs et simples. Autrement dit, l'information doit être présentée de manière efficace et succincte pour **ne pas être noyée** parmi d'autres contenus informatifs.

**Exemple**

Une entreprise ne respecte pas l'exigence d'accessibilité de l'information lorsqu'elle multiplie les pages à consulter, les liens présents dans les différentes pages et la redondance des informations.
La forme de présentation doit **tenir compte du support** sur lequel est communiquée l'information. Par exemple, pour éviter des mentions trop longues au niveau d'un formulaire en ligne, le responsable du traitement peut donner un premier niveau d'information en fin de formulaire et renvoyer vers une page dédiée sur son site internet.
Le titre de la page doit être clair, par exemple : « politique de confidentialité », « page vie privée » ou « données personnelles ». Cette page fait partie des mentions obligatoires sur un site internet.

**À noter**

La Cnil met à disposition de nombreux exemples de mentions d'information, applicables selon la situation (ex : vente en ligne, prospection commerciale, vidéosurveillance sur le lieu de travail, accès aux locaux professionnels par badge).

**Quelle sanction en l'absence d'information ?**

Le fait de ne pas informer la personne auprès de laquelle sont recueillies des données est puni d'une **amende pénale** de 1 500 € pour les entrepreneurs individuels et 7 500 € pour les sociétés.

## Recueillir le consentement des personnes concernées

Le **consentement** correspond à toute manifestation de volonté par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.
Le plus souvent, le responsable du traitement doit **recueillir le consentement** de la personne avant de mettre en œuvre le traitement de ses données personnelles.

**Le recueil de consentement est-il toujours obligatoire ?**

Le recueil du consentement est **obligatoire**, à moins que le traitement soit justifié par **l'exécution d'un contrat** (ex : contrat de travail, contrat de vente, de location).
De plus, le recueil de consentement est **toujours obligatoire** dans les cas suivants :
Collecte de **données personnelles « sensibles »**. Il s'agit d'une catégorie de données éminemment personnelles qui sont susceptibles de conduire à des discriminations si elles sont révélées (ex : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, orientation sexuelle, appartenance syndicale, données génétiques).
Réutilisation des données pour **d'autres finalités**. Par exemple, un magasin de sport organise un concours et collecte les données des participants pour pouvoir contacter le gagnant (finalité initiale). Si le magasin décide, par la suite, d'utiliser ces données pour constituer un fichier client (nouvelle finalité), il devra de nouveau recueillir le consentement des personnes.
Utilisation de **cookies non essentiels** au fonctionnement du service (ex : ciblage publicitaire). La Cnil a constitué un dossier sur les règles applicables à l'usage de cookies.
Utilisation des données à des fins de **prospection commerciale** par voie électronique (ex : newsletter, sms).
L'obligation de consentement s'éteint si la personne prospectée est déjà cliente de l'entreprise et que la prospection concerne des produits ou services similaires.

**Comment recueillir un consentement valable ?**

Pour être valable, le consentement obtenu doit remplir les **4 conditions suivantes** :
Le consentement doit être **libre** : il ne doit être ni contraint ni influencé. La personne concernée doit avoir véritablement le choix d'accepter ou de refuser le traitement, sans avoir à subir de conséquences négatives en cas de refus (ex : inaccessibilité du site internet). La personne doit également avoir le droit de retirer son consentement à tout moment, et aussi facilement qu'elle l'a donné.
Le consentement doit être **éclairé** : avant de consentir, la personne concernée doit avoir reçu une information suffisante (identité du responsable du traitement, finalité du traitement, type de données collectées, droit de retirer le consentement et éventuel transfert des données hors UE) de manière à pouvoir décider en toute connaissance de cause. L'information doit être communiquée en des termes clairs et facilement compréhensibles.
Le consentement doit être **spécifique** : si le traitement comporte plusieurs finalités (ex : gestion de clientèle, enquête de satisfaction, opération de prospection), la personne concernée doit pouvoir donner son consentement de façon indépendante pour l'une ou l'autre de ces finalités.
Le consentement doit être **univoque** : il doit être donné par un acte délibéré, sans aucune ambiguïté. Il peut être recueilli, par exemple, au moyen d'une déclaration écrite ou orale ou via le cochage d'une case par voie électronique (ex : « J'accepte que mon adresse électronique soit réutilisée à des fins de prospection commerciale par courrier électronique ».
En revanche, l'utilisation de cases de consentement cochées par défaut est **interdite**. De plus, le silence de la personne concernée (ex : la personne visite le site internet sans accepter ou refuser les cookies) **ne vaut pas consentement**.

**À noter**

Le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement libre, éclairé, spécifique et univoque.

**Comment fonctionne le retrait du consentement ?**

La personne concernée doit également avoir le **droit de retirer son consentement** à tout moment, et aussi facilement qu'elle l'a donné. Par exemple, lorsque le consentement est obtenu par voie électronique uniquement par un clic, une frappe ou en balayant l'écran, la personne concernée doit pouvoir retirer ce consentement de la même manière.

**Exemple**

Le fait d'obliger la personne concernée à suivre un cheminement complexe via des liens vers des documents électroniques ou le fait de la contraindre à saisir un mot de passe ne respecte pas l'exigence de pouvoir retirer son consentement de manière aussi simple qu'on l'a donné.

Lorsqu'une personne concernée retire son consentement, le responsable du traitement doit cesser tous les traitements qui se fondent sur celui-ci. Toutefois, les opérations réalisées sur la base d'un consentement donné valablement avant le retrait restent valables.

**Quelle sanction en l'absence de consentement ?**

Lorsque le recueil de consentement est obligatoire, le traitement de données personnelles obtenues **sans le consentement** de la personne concernée est puni pénalement de **5 ans** d'emprisonnement et 300 000 € d'amende pour les entrepreneurs individuels et 1 500 000 € pour les sociétés.

## Garantir les droits des personnes concernées

Le responsable du traitement doit **garantir des droits** aux personnes dont les données sont collectées : droit d'accès, droit de rectification, droit d'effacement, droit à la portabilité des données ainsi que le droit d'opposition au traitement.

**Droit d'accès aux données**

Le responsable du traitement doit permettre, à la personne qui en fait la demande, **d'accéder à ses données** faisant l'objet d'un traitement. La personne concernée doit pouvoir exercer ce droit, par exemple, au moyen d'un formulaire en ligne, d'une messagerie ou d'un mail de contact.

À cette occasion, le responsable doit lui fournir les **informations suivantes** :

Finalité poursuivie par le traitement : c'est-à-dire à quoi vont servir les données personnelles collectées

Destinataires des données personnelles : qui va recevoir et accéder aux données (service interne compétent, prestataire, etc.)

Durée de conservation des données personnelles

Droits de la personne sur ses données : droit de refuser le traitement, droit de rectifier et d'effacer ses données

Droit de la personne d'introduire une réclamation auprès de la Cnil

Source d'où proviennent les données personnelles, en cas de collecte indirecte

Existence d'un transfert des données personnelles vers un pays hors de lUnion européenne, le cas échéant.

La personne concernée doit pouvoir accéder aux informations sur lesquelles le responsable du traitement s'est fondé **pour prendre une décision la concernant**. Par exemple, les éléments qui auraient servi à un employeur pour ne pas lui accorder une promotion ou le score attribué par une banque et qui a conduit au rejet d'une demande de crédit.

Le responsable a **1 mois pour répondre** à compter de la date de réception de la demande, y compris s'il ne dispose d'aucune donnée sur la personne qui exerce son droit d'accès.

Les éléments doivent être communiqués **gratuitement** et de manière **facilement compréhensible**. Les codes, sigles et abréviations utilisés doivent être expliqués (éventuellement par le biais d'un lexique).

**Exemple**

Le code « Segmentation : A+ » peut signifier que la personne concernée est considérée comme un client VIP.

Le responsable du traitement peut **refuser la demande d'accès** à condition de motiver sa décision. Dans ce cas, il doit informer le demandeur des voies et délais de recours permettant de la contester.

Il peut également **ne pas répondre aux demandes manifestement abusives** notamment en raison de leur nombre et de leur caractère répétitif ou systématique (ex : demande d'une copie intégrale d'un enregistrement toutes les semaines).

**Droit de rectification des données**

Le responsable du traitement doit permettre, à la personne qui en fait la demande, de **rectifier ses données inexactes** dans les meilleurs délais. La personne concernée doit pouvoir compléter ses données incomplètes, y compris en fournissant une déclaration complémentaire.

**Droit à l'effacement des données (« droit à l'oubli »)**

Le responsable du traitement doit permettre, à la personne qui en fait la demande, d'obtenir **l'effacement de ses données** dans les meilleurs délais.

Ce « droit à l'oubli » n'est pas général, il s'applique **uniquement dans les cas suivants** :

Les données personnelles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière.
La personne concernée retire le consentement sur lequel est fondé le traitement, et ce traitement n'est pas justifié par l'exécution d'un contrat (ex : contrat de vente, de location, de travail).
La personne concernée s'oppose au traitement et il n'existe pas de motif légitime pour le traitement.
Les données personnelles ont fait l'objet d'un traitement illicite (ex : le consentement de la personne n'a pas été reucueilli alors qu'il était obligatoire)
Les données personnelles doivent être effacées pour respecter une obligation légale prévue par le droit de l'UE ou par le droit de l'État membre auquel le responsable du traitement est soumis.

**Droit à la portabilité des données**

Le responsable du traitement doit permettre, à la personne qui en fait la demande, **de recevoir ses données et de les réutiliser**, dans un délai raisonnable (entre 1 et 3 mois selon la complexité de la demande).
Le droit à la portabilité s'applique aux données personnelles **déclarées par la personne** (ex : adresse mail, nom, âge) ainsi qu'à celles **générées par son activité** lorsqu'elle utilise un service ou un appareil (ex : achats enregistrés sur une carte de fidélité).
En revanche, les données personnelles qui sont **dérivées, calculées ou déduites** à partir des données fournies par la personne concernée (ex : profilage à des fins publicitaires) ne rentrent pas dans le périmètre de ce droit.

**À noter**

Par ailleurs, ce droit concerne uniquement les données traitées à l'aide de procédés automatisés, ce qui exclut les données conservées sous format papier.
Le responsable doit communiquer **gratuitement** les données dans un **format structuré, couramment utilisé et lisible par ordinateur**. Lorsque c'est techniquement possible, la personne peut demander à ce que ses données soient directement transmises à un autre responsable de traitement.
Ce droit n'entraîne pas la suppression des données du service depuis lequel elles sont portées. De plus, il peut s'exercer à tout moment, y compris si la personne veut continuer à utiliser le service après avoir exercé ce droit.

**Exemple**

Le droit à la portabilité peut être exercé dans de nombreuses situations, par exemple :
Services de musique ou de vidéo à la demande (ex : listes de lecture, contenus téléchargés)
Réseaux sociaux (ex : liste des messages et des interactions)
Sites de e-commerce (ex : adresse, numéro de téléphone)
Ouverture et gestion d'un compte bancaire (ex : numéro de téléphone, liste de transactions réalisées)
Services de messagerie en ligne (ex : numéro de téléphone, adresse courriel de récupération)
La Cnil recommande fortement de mettre en place une procédure interne pour répondre aux demandes qui pourraient être reçues. Par exemple, prévoir une fonctionnalité permettant à la personne concernée de télécharger ses données dans un format standard lisible par un ordinateur (CSV, XML, JSON, etc.) directement depuis son compte/espace authentifié.
Le responsable du traitement peut **refuser la demande de portabilité** à condition de motiver sa décision. Il peut également **ne pas répondre aux demandes manifestement abusives** notamment en raison de leur nombre et de leur caractère répétitif ou systématique.

**Droit d'opposition au traitement**

Le responsable du traitement doit permettre à la personne concernée de **s'opposer à la réutilisation de ses données** à des fins de sollicitations, notamment commerciales, lors d'une commande ou de la signature d'un contrat.
Une case à cocher, non cochée par défaut, doit leur permettre d'exprimer leur choix directement sur le formulaire ou le bon de commande à remplir. La simple mention de l'existence de ce droit dans les conditions générales n'est pas suffisante.
Le droit d'opposition peut être exercé par la personne **seulement si** le traitement est justifié par un intérêt légitime (ex : traitement mis en œuvre à des fins de prévention de la fraude ou visant à garantir la sécurité du réseau et des informations).
Au contraire, si le traitement est justifié parce que la personne concernée a donné son consentement, celle-ci devra exercer son droit au retrait du consentement et pas son droit d'opposition.

## Tenir un registre des traitements

Le registre des activités de traitement permet de **recenser les traitements de données** et d'avoir d'une vue d'ensemble des utlisations de ces données personnelles.

**Qui est concerné par le registre ?**

L'obligation de tenir un registre des traitements ne s'applique pas à toutes les entreprises, il est nécessaire de se référer à leur taille.
La tenue du registre est **obligatoire** lorsque l'entreprise procède à **l'un des traitements suivants** :

Traitement **non occasionnel** (ex : gestion de la paie, gestion des clients/prospects et des fournisseurs)
Traitement susceptible de comporter un **risque pour les droits et libertés des personnes** (ex : systèmes de géolocalisation, de vidéosurveillance)
Traitement portant sur des **données sensibles** ou des données relatives à des **condamnations pénales**.
En cas de doute, la Cnil recommande d''intégrer le traitement dans le registre.
Lorsque l'entreprise emploie au moins 250 salariés, la tenue d'un registre des traitements est **obligatoire**.

**À noter**

Les **sous-traitants** doivent également tenir un registre de leurs activités impliquant le traitement de données.

**Que doit contenir le registre ?**

Le registre doit **recenser l'ensemble des traitements** mis en œuvre par l'entreprise.
En pratique, une fiche de registre doit être établie pour chaque traitement. Chaque fiche de registre doit contenir les **éléments suivants** :
Identité du responsable de traitement, du délégué à la protection des données et des sous-traitants
Catégories de personnes concernées (ex : client, prospect, employé)
Catégories de données traitées (ex : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation)
Finalités du traitement, c'est-à-dire l'objectif en vue duquel ces données ont été collectées
Destinataires des données, c'est-à-dire ceux à qui les données ont été ou seront communiquées, y compris les sous-traitants
Durée de conservation des données, ou à défaut les critères permettant de la déterminer
Description générale des mesures de sécurité des données
Le cas échéant, transfert des données vers un pays hors de lUE.

**Quelle forme doit prendre le registre ?**

Le RGPD impose uniquement que **le registre se présente sous une forme écrite** Le format du registre est libre et peut être constitué au format papier ou électronique.
La CNIL met à disposition des modèles de registre de traitement.

## Assurer la sécurité des données personnelles

Toute entreprise doit **assurer la sécurité des données personnelles** qu'elle a collectées (données de clients, de fournisseurs, d'employés, etc.). Pour garantir un niveau de sécurité adapté au risque, de nombreuses **mesures techniques et organisationnelles** sont nécessaires.

**À savoir**

La Cnil met à disposition un guide pratique sur la sécurisation des données.

**Recenser les traitements de données**

Le responsable du traitement doit **recenser les traitements** de données personnelles (automatisés ou non) **et les supports** sur lesquels ces traitements reposent, c'est-à-dire :
les matériels (ex. : serveurs, ordinateurs portables, disques durs)
les logiciels (ex. : systèmes d'exploitation, logiciels métier)
les canaux de communication logiques ou physiques (ex. : fibre optique, Wi-Fi, Internet, échanges verbaux, coursiers)
les supports papier (ex. : documents imprimés, photocopies)
les locaux et installations physiques où se situent les éléments précédemment cités (ex. : locaux informatiques, bureaux).

**Apprécier les risques liés à chaque traitement**

Ce recensement permet d'**apprécier les risques** engendrés par chaque traitement, notamment :
**Accès illégitime à des données** (ex : usurpation d'identité consécutive à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise)
**Modification non désirée de données** (ex : accusation à tort d'une personne d'une faute ou d'un délit suite à la modification de journaux d'accès)
**Disparition de données** (ex : non-détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient).
Le responsable du traitement doit identifier les **sources de risques** en prenant en compte des sources humaines (ex : administrateur informatique, utilisateur, attaquant externe, concurrent) et non humaines (ex : eau, épidémie, matériaux dangereux, virus informatique non ciblé).
Il doit également **estimer la gravité et la vraisemblance des risques** (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale) pour ainsi **déterminer les mesures** à même de traiter chaque risque (ex : contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation).

**Sensibiliser les utilisateurs**

Le responsable du traitement doit **sensibiliser** les utilisateurs sur les enjeux en matière de sécurité et de vie privée. Pour ce faire, il peut organiser une séance de sensibilisation, envoyer régulièrement les mises à jour des procédures pertinentes pour les personnes selon leurs fonctions, faire des rappels par messagerie électronique, etc.
Le responsable doit **documenter les procédures d'exploitation,** les tenir à jour et les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action sur un traitement de données personnelles, qu'il s'agisse d'une opération d'administration ou de la simple utilisation d'une application, doit être expliquée dans un langage clair et adapté à chaque catégorie d'utilisateurs, dans des documents auxquels ces derniers peuvent se référer.
De plus, il doit **rédiger une charte informatique**, annexée au règlement intérieur, comportant les informations suivantes :
Règles de protection des données et sanctions encourues en cas de manquement
Champ d'application de la charte (ex : modalités d'intervention des équipes chargées de la gestion des données, moyens d'authentification, règles de sécurité)
Modalités d'utilisation des moyens informatiques mis à disposition (poste de travail, espace de stockage, accès à internet, messagerie électronique…)
Conditions d'administration du système d'information
Responsabilités et sanctions encourues en cas de non respect de la charte.

**À noter**

Il peut être judicieux de prévoir la signature d'un**engagement de confidentialité**, ou de prévoir dans les contrats de travail une clause de confidentialité spécifique concernant les données personnelles. Un **modèle** d'engagement de confidentialité est mis à disposition par la Cnil.

**Modèle d'engagement de confidentialité sur les données**

Je soussigné/e Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____ (ci-après dénommée « la Société »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare
reconnaître la confidentialité desdites données.
Je m'engage par conséquent, conformément à l'article 32 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes à l'état de l'art et aux règles internes dans le cadre de mes attributions
afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.
Je m'engage en particulier à :
ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
prendre toutes les mesures conformes à l'état de l'art et aux règles internes dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
prendre toutes précautions conformes à l'état de l'art et aux règles internes pour préserver la sécurité physique et logique de ces données ;
m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.
Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée, après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation
et la communication de données à caractère personnel.
J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la règlementation en vigueur, notamment au regard des articles 226-13 et 226-16 à 226-24 du code pénal.
Fait à _____, le jj/mm/aaaa, en X exemplaires
Nom :
Signature :

**Authentifier les utilisateurs**

Pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un**identifiant qui lui est propre** et doit **s'authentifier** avant toute utilisation des moyens informatiques.
Une précaution indispensable consiste à **définir un identifiant unique par utilisateur** et interdire les comptes partagés entre plusieurs utilisateurs. Dans le cas où l'utilisation d'identifiants génériques ou partagés est incontournable, il est nécessaire de mettre œuvre les mesures suivantes :

Exiger une validation de la hiérarchie
Mettre en œuvre des moyens pour tracer les actions associées à ces identifiants
Renouveler le mot de passe dès qu'une personne n'a plus besoin d'accéder au compte.

**À noter**

En cas d'authentification des utilisateurs basée sur des mots de passe, il est conseillé de suivre les recommandations de la Cnil .

**Gérer l'habilitation des utilisateurs**

Le responsable du traitement doit **gérer l'habilitation des utilisateurs** afin de limiter leur accès aux seules données dont ils ont besoin pour l'accomplissement de leurs missions.
Le responsable est d'abord amené à **définir des profils d'habilitation** dans les systèmes en séparant les tâches et les domaines de responsabilité et **faire valider toute demande d'habilitation** par un responsable (ex : supérieur hiérarchique, chef de projet).
Il est impératif de **supprimer les permissions d'accès** des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique (ex : changement de mission ou de poste), ainsi qu'à la fin de leur contrat.

**À noter**

Il est recommandé de **réaliser une revue régulière des habilitations** (au moins une fois par an) pour identifier et supprimer les comptes non utilisés et réaligner les droits accordés sur les fonctions de chaque utilisateur.

**Tracer les opérations**

Le responsable du traitement doit également **tracer les opérations** afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).
Pour ce faire, il est nécessaire de mettre en place **un système de journalisation**, c'est-à-dire un enregistrement des activités métier des utilisateurs, des interventions techniques (y compris par les administrateurs), des anomalies et des événements liés à la sécurité.
Le responsable du traitement doit s'assurer que les gestionnaires de l'enregistrement des opérations lui notifient toute anomalie ou tout incident de sécurité, dans les plus brefs délais.

**À noter**

L' Anssi met à disposition un guide des bonnes pratiques pour établir un système de journalisation efficace et sécurisé.

**Sécuriser les postes de travail et l'informatique mobile**

Les risques d'intrusion dans les systèmes informatiques sont importants. Le responsable du traitement doit **protéger les postes de travail** qui constituent un des principaux points d'entrée.
Afin de prévenir les accès frauduleux, l'exécution de virus ou les prises de contrôle malveillantes à distance, le responsable du traitement doit prendre les **précautions suivantes** :
Prévoir un mécanisme de **verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné
Installer un **« pare-feu »** (« firewall ») logiciel sur le poste et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail
Utiliser des **antivirus régulièrement mis à jour** et prévoir une politique de **mise à jour régulière des logiciels**
Effacer de façon sécurisée les données présentes sur un poste **avant sa réaffectation** à une autre personne.

**À noter**

Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) détaille les bons réflexes à adopter en cas d'intrusion sur un système d'information.
Les pratiques de travail hors des locaux (ex : déplacements, télétravail) comportent des risques spécifiques liés à l'usage d'ordinateurs portables, de clés USB ou encore de smartphones. Il est donc indispensable d'anticiper l'atteinte à la sécurité des données **à l'extérieur des locaux**.
Le responsable du traitement doit **sensibiliser les utilisateurs** aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles (ex : vol de matériel, risques liés à la connexion aux réseaux publics) et **imposer l'utilisation d'un VPN** à authentification forte.
Il est également recommandé de **prévoir des moyens de chiffrement** des postes nomades et des supports de stockage mobiles (ex : ordinateur portable, clés USB, disque dur externes, CD-R, DVD-RW), tels que :
Le chiffrement du disque dur (de nombreux systèmes d'exploitation intègrent une telle fonctionnalité)
Le chiffrement fichier par fichier
La création de conteneurs (fichier susceptible de contenir plusieurs fichiers) chiffrés.

**À noter**

La CNIL rappelle les grands principes de la cryptologie (chiffrement, hachage, signature).

**Sauvegarder et archiver les données**

Le responsable du traitement doit **effectuer des sauvegardes régulières** pour limiter l'impact d'une disparition ou d'une altération non désirée de données. Il est également recommandé de stocker au moins une **sauvegarde sur un site extérieur** et d'isoler une **sauvegarde hors ligne**, déconnectée du réseau de l'entreprise.

Par ailleurs, le responsable doit **archiver les données qui ne sont plus utilisées au quotidien** mais qui n'ont pas encore atteint leur durée limite de conservation, par exemple parce qu'elles sont conservées afin d'être utilisées en cas de litige.
Pour ce faire, il doit définir un processus de gestion des archives qui appelent plusieurs questions, notamment :
Quelles données doivent être archivées ?
Comment et où sont-elles stockées ?
Quelles sont les modalités d'accès spécifiques aux données archivées ? (l'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle)
S'agissant de la destruction des archives, quel mode opératoire faut-il choisir pour garantir que l'intégralité d'une archive a été détruite ?

**À noter**

La CNIL a établi une liste de recommandations concernant les modalités d'archivage électronique.

**Gérer la sous-traitance**

Les traitements de données réalisés par un sous-traitant pour le compte du responsable de traitement doivent bénéficier de garanties suffisantes, notamment en matière de sécurité.
Il est impératif de faire appel uniquement à des **sous-traitants présentant des garanties suffisantes**, notamment en termes de connaissances spécialisées, de fiabilité et de ressources. Le responsable doit exiger la communication par le prestataire de sa politique de sécurité des systèmes d'information et de ses éventuelles certifications.
Un contrat de sous-traitance doit définir l'objet, la durée, la finalité du traitement ainsi que les obligations des parties, notamment en termes de sécurité des traitements. Il doit contenir des dispositions fixant les éléments suivants :
Répartition des responsabilités et des obligations en matière de **confidentialité des données personnelles** confiées
**Contraintes minimales en matière d'authentification** des utilisateurs
**Conditions de restitution et de destruction des données** en fin du contrat
**Règles de gestion et de notification des incidents**. Celles-ci doit comprendre une information du responsable de traitement en cas de découverte de faille de sécurité ou d'incident de sécurité.

**À noter**

La CNIL a publié un guide pour accompagner les sous-traitants dans la mise en oeuvre concrète de leurs obligations.

**Évaluer la sécurité des données**

Les mesures permettant de garantir la sécurité des données étant nombreuses, il est opportun d'**évaluer le niveau de sécurité des données personnelles** de l'entreprise. La CNIL met à disposition une grille d'évaluation .
Les mesures techniques et organisationnelles mises en œuvre par le responsable de traitement doivent être **appropriées**, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques (dont le degré de probabilité et de gravité varie) pour les droits et libertés des personnes.
En cas de violation de données (ex : divulgation non autorisée, accès irrégulier), le responsable de traitement doit être **en mesure de prouver** qu'il a pris les mesures de sécurité adéquates.

## Encadrer la sous-traitance

Le responsable de traitement peut **recourir à un sous-traitant** chargé de traiter les données personnelles pour son compte.
Il peut s'agir d'un prestataire de service informatique (ex : hébergement, maintenance), d'une entreprise de sécurité informatique voire d'une agence de marketing ou de communication traitant les données personnelles pour le compte du responsable de traitement.
Pour encadrer leur relation, le responsable de traitement et son sous-traitant doivent conclure un **contrat de sous-traitance**.

**Quelles mentions doivent figurer dans le contrat ?**

Le responsable de traitement et le sous-traitant doivent conclure un contrat incluant les **mentions obligatoires suivantes** :
Objet du contrat, c'est-à-dire l'activité du sous-traitant (ex : hébergement de données, routage d'emails, maintenance)
Nature, finalité et durée du traitement
Type de données personnelles collectées et catégories de personnes concernées
Obligations et droits du responsable du traitement
Obligations et droits du sous-traitant.
Pour faciliter la rédaction de ce contrat, les parties peuvent y insérer certaines clauses contractuelles types (CCT) rédigées par la Commission européenne. Elles fournissent un support utile pour encadrer la sous-traitance conformément aux exigences du RGPD.

**À noter**

Toute opération de traitement non prévue dans le contrat doit, en principe, faire l'objet d'une renégociation préalable entre les parties ou au moins d'instructions écrites du responsable de traitement.

**Quelles sont les obligations du sous-traitant ?**
Le sous-traitant doit respecter les **obligations suivantes** :
Assurer un niveau de sécurité suffisant au regard de la nature des données traitées
Conseiller le responsable de traitement (ex : l'alerter s'il estime qu'une instruction qu'il reçoit constitue une violation de la réglementation applicable)
Aider le responsable de traitement à garantir les droits des personnes (accès, rectification, effacement, portabilité)
Formaliser à l'écrit les instructions délivrées par le responsable de traitement
Tenir un registre des activités de traitement effectuées pour le compte du responsable de traitement
Tenir à disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et permettre la réalisation d'audits
Veiller à ce que les personnes autorisées à traiter les données personnelles s'engagent à respecter la confidentialité.
**Registre tenu par le sous-traitant**
Le sous-traitant doit **tenir son propre registre**, recensant toutes les catégories d'activité de traitement effectuées pour le compte de ses clients (ex : hébergement de données, maintenance informatique, service d'envoi de messages de prospection commerciale).
En pratique, une fiche de registre doit être établie pour chacune de ces catégories d'activités. Chaque fiche de registre doit contenir les **éléments suivants** :
Identité du sous-traitant, de son représentant en cas d'établissement hors UE, de son délégué à la protection de données ainsi que les sous-traitants auxquels il a lui-même recours
Catégories de traitements effectués pour le compte de chacun de ses clients, c'est-à-dire les opérations effectivement réalisées pour leur compte. Par exemple, pour la catégorie « service d'envoi de messages de prospection », il peut s'agir de la collecte des adresses mails, de l'envoi sécurisé des messages, de la gestion des désabonnements, etc.)
Description générale des mesures de sécurité des données
Le cas échéant, transfert des données vers un pays hors de lUE.
**À noter**
La CNIL met à disposition un guide pratique à destination des sous-traitants.
**Le sous-traitant peut-il recourir lui-même à un sous-traitant ?**
Le sous-traitant doit **obtenir l'autorisation écrite** du responsable de traitement avant de recruter un autre sous-traitant. Cette autorisation peut être donnée au sous-traitant **au cas par cas** pour chaque nouveau sous-traitant, ou avoir une **portée générale**.
La CNIL recommande de préciser dans le contrat laquelle de ces 2 modalités d'autorisation est choisie par les parties.
Si l'autorisation a une portée générale, le sous-traitant doit communiquer au responsable de traitement de la **liste de ses sous-traitants ultérieurs**, ainsi que tout ajout ou remplacement dans cette liste pour lui permettre de s'y opposer s'il le souhaite. Dans ce cas, la Cnil recommande de formaliser les modalités d'information du responsable de traitement et, éventuellement, les critères du choix de ces sous-traitants.
**À noter**
Le sous-traitant doit tenir à jour, dans son registre, une liste des sous-traitants auxquels il recourt.

## Désigner un délégué à la protection des données (DPO)

Les entreprises réalisant des traitement de données à grande échelle doivent désigner un **délégué à la protection des données**, appelé le plus souvent « data protection officer (DPO) » en anglais. Le DPO est chargé d'**assurer la protection des données personnelles** collectées et traitées par l'entreprise qui l'emploie.
**À noter**
La CNIL met à disposition un guide pratique du DPO .
**La désignation d'un DPO est-elle obligatoire ?**
La désignation d'un DPO par l'entreprise est **obligatoire** dans **les 2 cas suivants** :
Les activités principales de l'entreprise ou du sous-traitant impliquent un **suivi régulier et systématique à grande échelle** des personnes concernées par les opérations de traitement (ex : géolocalisation, vidéosurveillance, traitement des échanges bancaires).
Les activités principales de l'entreprise ou du sous-traitant impliquent un **traitement à grande échelle de données sensibles** ou relatives à des condamnations pénales.
La notion de traitement « **à grande échelle** » s'analyse au cas par cas, en fonction du nombre de personnes concernées, du volume et de l'éventail des différentes données collectées, de la durée de l'activité de traitement et de la répartition géographique de l'activité de traitement.
**Exemple**
**Quelques exemples de traitements à grande échelle :**

le traitement à des fins statistiques de données de localisation actuelles de clients d'une chaîne de restauration rapide internationale par un sous-traitant spécialisé dans ces services
le traitement de données de clients dans le cadre des activités courantes d'une compagnie d'assurance ou d'une banque
le traitement de données personnelles par un moteur de recherche en vue de l'affichage de publicités sur la base du comportement de navigation
le traitement de données personnelles (contenu, flux des données, localisation) par des fournisseurs de services de téléphonie et d'Internet.

**À l'inverse, des exemples de traitements qui ne sont pas considérés comme des traitements à grande échelle :**

le traitement de données de patients par un médecin indépendant
le traitement de données personnelles relatives à des condamnations par un avocat.

**À noter**

En dehors des cas de désignation obligatoire, la désignation d'un délégué à la protection des données est **encouragée**.

**Quelles sont les missions du DPO ?**

Les missions du délégué à la protection des données sont les suivantes :

**Informer et conseiller** le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent

**Contrôler** le respect du RGPD et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement

**Dispenser des conseils et recommandations**, sur demande, sur un sujet précis en lien avec le traitement des données personnelles

**Coopérer avec la Cnil** et faire office de point de contact sur les questions relatives au traitement.

**À noter**

Le délégué à la protection des données est soumis à une **obligation de confidentialité** en ce qui concerne l'exercice de ses missions.

**Comment choisir et désigner le DPO ?**

Le responsable de traitement peut désigner un DPO **en interne** ou un **prestataire externe** proposant ses services de DPO. Il doit s'assurer que le DPO dispose de **connaissances spécialisées** du droit et des pratiques en matière de protection des données. Il doit prendre en compte les formations suivies par la personne pressentie, ainsi que son **expérience** et sa connaissance du secteur.

La Cnil a mis en place une **procédure de certification** des compétences du DPO. La procédure n'est **pas obligatoire** mais permet au DPO l'ayant suivie de justifier qu'il répond aux exigences de compétences. Les certifications sont délivrées par des organismes certificateurs agréés par la CNIL.

**À noter**

Pour vérifier qu'un DPO est véritablement certifié, le responsable de traitement peut contacter l'organisme ayant attribué la certification. La CNIL publie une liste des organismes de certification agréés .

Lorsqu'il a choisi le DPO de l'entreprise, le responsable de traitement doit remplir le **formulaire de désignation en ligne** pour en informer la CNIL.

- Désignation d'un délégué à la protection des données (DPO)

**Quelles sont les conditions d'exercice de la fonction de DPO ?**

Le responsable du traitement doit permettre au DPO d'exercer ses missions de contrôle, de conseil et de point de contact **en toute indépendance**. L'indépendance doit être garantie de la manière suivante :

Le DPO ne doit pas être en situation de conflit d'intérêts en cas de cumul de sa fonction de DPO avec une autre fonction. Par exemple, il y a conflit d'intérêts lorsque le DPO se voit confier des missions dans lesquelles il détermine les finalités et les moyens du traitement.

Le DPO doit pouvoir rendre compte de son action au plus haut niveau de la direction de l'entreprise

Le DPO ne pas être sanctionné pour l'exercice de ses missions de DPO

Le DPO ne doit pas recevoir d'instruction dans le cadre de l'exercice de ses missions de DPO.

De plus, le DPO doit disposer du temps suffisant ainsi que des **moyens matériels et humains adéquats** pour exercer sa mission. Il doit bénéficier du soutien actif de la direction et être **associé en amont à tous les projets** impliquant des données personnelles.

**À noter**

Le DPO peut exercer sa fonction de délégué **à temps partiel**, en complément d'autres activités pour l'organisme (en interne) ou pour d'autres clients (en externe).

**Que risque l'entreprise qui ne désigne pas de DPO ?**

Une entreprise qui ne désigne pas DPO lorsque cette désignation est obligatoire s'expose aux **sanctions de la Cnil** :

Rappel à l'ordre
Injonction à se mettre en conformité
Amende administrative pouvant s'élever jusqu'à **10 millions d'euros** ou 2 % **du chiffre d'affaires annuel** mondial de l'exercice précédent, le montant le plus élevé étant retenu.

## Réaliser une analyse d'impact

Pour s'assurer de la conformité de son traitement au RGPD, l'entreprise peut être amenée à réaliser une**analyse d'impact relative à la protection des données (AIPD)**. Cette procédure permet d'évaluer à la fois les risques encourus et la manière dont ils peuvent être maîtrisés.

**L'analyse d'impact est-elle obligatoire ?**

La réalisation d'une analyse d'impact est **obligatoire** lorsque le traitement de données présente un**risque élevé pour les droits et libertés** des personnes concernées, c'est-à-dire :

Soit le traitement figure dans la liste des traitements pour lesquels la CNIL a estimé obligatoire de réaliser une analyse d'impact.

Soit le traitement remplit au moins **2 des critères suivants** :

évaluation/scoring (y compris le profilage)
décision automatique avec effet légal ou similaire
surveillance systématique
collecte de données sensibles
collecte de données personnelles à large échelle
croisement de données
personnes vulnérables (patients, personnes âgées, enfants, etc.)
usage innovant (utilisation d'une nouvelle technologie)
exclusion du bénéfice d'un droit/contrat.

**Exemple**

Une entreprise met en place un traitement publicitaire visant à collecter les données de géolocalisation de plusieurs millions d'individus pour créer des profils publicitaires et leur afficher de la publicité ciblée en fonction de leurs déplacements.

Ce traitement remplit le critère de la collecte à grande échelle et celui de la collecte de données sensibles (données de localisation). Ainsi, la réalisation d'une AIPD sera nécessaire.

L'AIPD doit être menée **avant la mise en œuvre du traitement** Elle doit être démarrée le plus en amont possible et sera mise à jour tout au long du cycle de vie du traitement.

**Que doit contenir l'analyse d'impact ?**

L'analyse d'impact doit contenir au minimum les **informations suivantes** :

**Description** systématique des **opérations de traitement** envisagées et les **finalités** du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement

**Évaluation de la nécessité** et de la **proportionnalité** des opérations de traitement au regard des finalités

**Évaluation des risques** sur les droits et libertés des personnes concernées

**Mesures envisagées** pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données personnelles et à apporter la preuve du respect du règlement.

**À noter**

La Cnil met à disposition des guides de bonnes pratiques ainsi qu'un logiciel gratuit pour faciliter la réalisation d'une analyse d'impact.

Le responsable du traitement doit ensuite **transmettre l'analyse d'impact à la Cnil** au moyen du service en ligne suivant :

- Soumettre une analyse d'impact relative à la protection des données (AIPD) à la CNIL

**Quelles sanctions en l'absence d'analyse d'impact ?**

Une entreprise qui ne réalise pas d'analyse d'impact s'expose aux**sanctions de la Cnil** :

Rappel à l'ordre
Injonction à se mettre en conformité
Amende administrative pouvant s'élever jusqu'à **10 millions d'euros** ou 2 % **du chiffre d'affaires annuel** mondial de l'exercice précédent, le montant le plus élevé étant retenu.

## Protéger les données en cas de transfert hors de l'UE

Le transfert de données hors de l'UE consiste pour une entreprise à envoyer des données personnelles qu'elle a collectées **vers un pays non membre de l'Union européenne (UE)**.

Le plus souvent, un transfert de données hors UE a lieu dans les**2 cas suivants** :

**L'entreprise a recours à un sous-traitant établi hors de l'UE** (ex : un hébergeur de données établi aux États-Unis)
**Les entreprises d'un même groupe échangent des données** (ex : la filiale française envoie les données personnelles de ses salariés au siège du groupe situé au Japon).

**À quelles conditions les données peuvent-elles être transférées hors UE ?**

Pour qu'un transfert de données hors de l'UE soit autorisé, le pays recevant les données doit faire l'objet d'une **décision d'adéquation**.

Il s'agit d'une décision adoptée par la Commission européenne qui établit qu'un pays tier présente un **niveau de protection adéquat** des données personnelles. La Commission évalue ce niveau de protection à partir d'éléments fixés par le RGPD (ex : la législation interne du pays, l'existence d'une autorité de contrôle indépendante en matière de protection des données et les engagements internationaux pris par le pays).

La décision d'adéquation a pour effet de permettre le transfert de données vers le pays concerné, **sans exigences supplémentaires**.

**À noter**

Le transfert de données est **libre**, par exemple, vers le Royaume-Uni, le Japon, l'Argentine, la Corée du Sud ou les États-Unis (vers les entités américaines certifiées). La liste des pays adéquats est accessible sur le site de la CNIL.

En l'absence de décision d'adéquation, le responsable de traitement doit mettre en place des «**garanties appropriées** » avant de transférer les données hors de l'UE. Il peut s'agir des garanties suivantes :

Conclure un contrat incluant des clauses contractuelles types (CCT) de la Commission européenne. Ces clauses fournissent un support utile pour encadrer le transfert hors UE, conformément aux exigences du RGPD.

Établir des **règles d'entreprise contraignantes** ( Binding Corporate Rules (BCR) en anglais). Pour les multinationales effectuant de nombreux transfert de données, ces règles désignent une politique de protection des données intra-groupe permettant d'unifier les garanties concernant les traitements de données personnelles offertes par leurs filiales dans le monde entier.

Adhérer à un **code de conduite**. Le code est un outil mis en place par une organisation représentative d'un secteur d'activité. Il met en lumière les bonnes pratiques du secteur avec, par exemple, des mentions d'information type, des modèles de clauses contractuelles ou des préconisations en matière de mesures de sécurité, dans un vocabulaire adapté au secteur. Le code est juridiquement contraignant pour ses adhérents.

**À noter**

S'il existe un risque que ces garanties ne soient pas effectives, l'exportateur de données doit mettre en place des mesures supplémentaires afin d'assurer l'effectivité des garanties.

**Quelles dérogations permettent de transférer les données hors UE ?**

En l'absence de décision d'adéquation ou de garanties appropriées, le transfert peut être réalisé **par dérogation**, dans des situations particulières :

La personne concernée a donné son **consentement explicite** au transfert envisagé, **après avoir été informée des risques que ce transfert pouvait comporter pour elle**

Le transfert est **nécessaire à l'exécution d'un contrat** entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à sa demande

Le transfert est **nécessaire à la conclusion ou à l'exécution d'un contratconclu dans l'intérêt de la personne concernée** entre le responsable du traitement et une autre personne physique ou morale

Le transfert est nécessaire pour des **motifs importants d'intérêt public**

Le transfert est nécessaire à **la constatation, à l'exercice ou à la défense de droits en justice**

Le transfert est **nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes**, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement

Le transfert a lieu **au départ d'un registre** qui est légalement destiné à fournir des informations au public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

**Transfert hors UE lorsqu'aucune situation particulière n'est applicable**

Lorsqu'aucune de ces situations n'est applicable, un transfert vers un pays tier est tout de même autorisé **si les conditions suivantes sont respectées** :

Le transfert n'a pas un caractère répétitif et ne touche qu'un nombre limité de personnes concernées

Le transfert est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée

Le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données personnelles.

**Gestion et protection des données**

**Pour en savoir plus**

- Guide RGPD pour les petites entreprises
  Source : Comité européen de la protection des données (CEPD)
- Exemples de mentions d'information (RGPD)
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Guide pratique pour la sécurisation des données
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Comment fonder un traitement sur l'intérêt légitime ?
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Modèles de registre de traitement de données
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Authentification par mot de passe (recommandations de la CNIL)
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Système de journalisation (recommandations de l'ANSSI)
  Source : Agence nationale de la sécurité des systèmes d'information (Anssi)
- Les bons réflexes en cas d'intrusion sur un système d'information
  Source : Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR)
- Modalités d'archivage électronique (recommandations de la CNIL)
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Grille d'évaluation du niveau de sécurité des données personnelles
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Guide du sous-traitant (RGPD)
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Clauses contractuelles types (sous-traitance et RGPD)
  Source : Commission européenne
- Guide pratique du DPO
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Liste des traitement pour lesquels une analyse d'impact est requise
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Réaliser une analyse d'impact – Guides pratiques
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Outil PIA en téléchargement : faciliter la conduite d'analyses d'impact
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Pays adéquats pour un transfert de données hors UE (RGPD)
  Source : Commission nationale de l'informatique et des libertés (Cnil)
- Clauses contractuelles types (transfert de données hors UE)
  Source : Commission européenne
- Fichier client et conformité au RGPD
  Source : France Num
- Règles à respecter pour le contrôle d'accès biométrique sur le lieu de travail
  Source : Commission nationale de l'informatique et des libertés (Cnil)

## Où s'informer ?

- **Commission nationale de l'informatique et des libertés (Cnil)**
  **Par courrier**
  3 Place de Fontenoy
  TSA 80715
  75334 Paris cedex 07
  La CNIL ne reçoit pas le public et n'assure aucun renseignement sur place.
  **Par téléphone**
  **+33 1 53 73 22 22**
  Accueil téléphonique ouvert du lundi au vendredi de 9h30 à 17h.
  Renseignements juridiques ouverts les lundi, mardi, jeudi et vendredi de 10h à 12h.
  **Par courriel**
  Accès au formulaire de contact

## Services en ligne

- Désignation d'un délégué à la protection des données (DPO)
  Téléservice
- Soumettre une analyse d'impact relative à la protection des données (AIPD) à la CNIL
  Téléservice
- Formation en ligne gratuite (RGPD – Atelier Mooc)
  Téléservice

**Textes de référence**

- Règlement (UE) 2016/679 du 27 avril 2016 – protection des personnes à l'égard du traitement des données personnelles (RGPD)
- Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Code de la consommation : articles L224-42-1 à L224-42-4
  Récupération et portabilité des données
- Code pénal : articles 226-16 à 226-24
  Sanctions pénales

*Luberon Monts de Vaucluse*
*Horaires : Lundi au vendredi de 8h30 à 12h00 et de 13h30 à 17h00*
*Adresse : 315 avenue Saint Baldou 84300 Cavaillon*
*Tél. : 04 90 78 82 30*