



L'ORGANISATION CONTRACTUELLE DES RELATIONS ENTRE LES ACTEURS DU TRAITEMENT

Fiche
n° 4

CE QU'IL FAUT RETENIR

Plusieurs acteurs peuvent être amenés à intervenir dans le cadre d'un traitement de données personnelles :

- ▶ **Le responsable du traitement** : il est à l'origine du traitement et en a déterminé les finalités et les moyens (le RGPD fait peser sur lui la plupart des responsabilités). Dans la majeure partie des cas, l'adhérent FFB est le responsable du traitement.
- ▶ **Le sous-traitant** : il réalise tout ou partie du traitement pour le compte du responsable du traitement dans le respect du contrat le liant à ce dernier (experts-comptables, prestataires de services informatiques, intégrateurs de logiciels, agences de communication ou de marketing, etc.).

Il faudra bien le choisir afin qu'il sécurise l'adhérent sur sa connaissance du RGPD et le respect de ses contraintes. En particulier, il faudra veiller à ce que le sous-traitant s'engage contractuellement à :

- ▶ Définir les modalités du traitement (objet, nature, durée, données concernées, etc.).
- ▶ Respecter la confidentialité des données.
- ▶ S'interdire de traiter les données sans instructions.
- ▶ Assurer la sécurité des données.
- ▶ S'interdire de recruter un autre sous-traitant sans autorisation préalable.
- ▶ Transférer à ses sous-traitants les obligations contractuelles de son propre contrat.
- ▶ Aider l'adhérent FFB à s'acquitter de ses obligations légales (information des personnes concernées et gestion de leurs demandes, analyses d'impact, registre de traitement, etc.).
- ▶ Supprimer ou restituer les données à l'issue du contrat.

Des clauses types sont annexées à la présente fiche.

Étapes à suivre pour l'adhérent FFB :

1. Identifier les traitements de données personnelles en cours au sein de la structure et les sous-traitants correspondants (voir l'annexe de la **fiche n° 1** pour la liste des traitements les plus courants).
2. Utiliser les clauses contractuelles ou les contrats types de la CNIL.
3. Contacter ses sous-traitants actuels et leur demander, si nécessaire, une mise à jour des contrats déjà signés.
4. Vérifier les CGV des prestataires proposant leurs services afin de s'assurer que les éléments obligatoires y figurent bien.
5. Formaliser des procédures d'échanges et de remontées d'information afin de faciliter le respect des obligations respectivement imposées aux acteurs du traitement.

L'ORGANISATION CONTRACTUELLE DES RELATIONS ENTRE LES ACTEURS DU TRAITEMENT

Fiche
n° 4

Plusieurs acteurs peuvent être amenés à intervenir dans le cadre d'un traitement de données personnelles.

Leurs prérogatives et responsabilités sont prévues par le règlement général sur la protection des données (RGPD), le texte allant même jusqu'à encadrer les relations contractuelles pouvant exister entre eux.

Rappel : qui sont les acteurs d'un traitement de données personnelles ?

L'acteur le plus déterminant du traitement de données personnelles est le **responsable du traitement**, c'est-à-dire « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, *détermine les finalités et les moyens du traitement* »¹.

En d'autres termes, le **responsable du traitement est à l'initiative du traitement** : il en a acté le principe ainsi que les contours et en a choisi les modalités d'exécution.

À ce titre, le RGPD place sur ses épaules la majeure partie des obligations liées à la protection des données (par exemple : informations des personnes concernées par le traitement, mise en œuvre des droits des personnes concernées, principe d'*accountability*, choix des sous-traitants, notification des personnes concernées et de la CNIL en cas de violation des données personnelles).



Dans la plupart des cas, les adhérents FFB seront des responsables du traitement !

Hypothèse : l'existence de plusieurs responsables de traitement

Le plus souvent, il n'y a qu'un seul responsable du traitement.

Cependant, le RGPD prévoit également l'hypothèse où plusieurs personnes déterminent les finalités et les moyens du traitement : dans ces circonstances, on parlera de « **responsables conjoints du traitement** »².

Les responsables conjoints définissent de manière transparente, par voie contractuelle, leurs obligations respectives, notamment en ce qui concerne la relation avec les personnes concernées (information sur les modalités du traitement et exercice de leurs droits).

Les grandes lignes de l'accord sont mises à la disposition des personnes fichées, celles-ci pouvant exercer leurs différents droits (accès, rectification, suppression, portabilité, etc.) envers chacun des responsables du traitement.

Pour la mise en place et l'exécution du traitement, le responsable du traitement peut avoir besoin d'une expertise extérieure : c'est là qu'intervient le **sous-traitant**³.

Au sens du RGPD, le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel *pour le compte du responsable du traitement* ».

En d'autres termes, le sous-traitant, au sens du RGPD⁴, est un exécutant :

- ▶ Il n'agit que sur instruction documentée du responsable du traitement.
- ▶ Il ne traite des données que pour le compte du responsable du traitement.
- ▶ Il ne peut agir que dans les limites de sa mission et du contrat qui le lie au responsable du traitement.

L'ORGANISATION CONTRACTUELLE DES RELATIONS ENTRE LES ACTEURS DU TRAITEMENT

Fiche
n° 4

Concrètement, qu'est-ce qu'un sous-traitant ?

La notion de « sous-traitant » peut convenir à un très grand nombre de prestataires : experts-comptables, prestataires de services informatiques (hébergement, maintenance, etc.), intégrateurs de logiciels, sociétés de sécurité informatique, entreprises de services du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) ou encore agences de marketing ou de communication traitant des données pour le compte de leurs clients.

À l'inverse, les éditeurs de logiciels ou les fabricants de matériels ne sont pas considérés comme des sous-traitants, à condition qu'ils n'aient pas accès et ne traitent pas les données collectées au moyen des équipements qu'ils vendent.

À noter que la nuance entre les notions de « responsables du traitement » et de « sous-traitants » peut parfois être ténue. En effet, il arrive souvent, surtout depuis l'émergence des géants du numérique (Microsoft, Salesforce.com, etc.), que le responsable du traitement ne fasse qu'utiliser une solution technique toute faite et sur laquelle il n'a aucune maîtrise. Les prestataires informatiques préciseront donc dans leurs conditions générales de vente qu'ils sont « sous-traitants » au sens de la réglementation applicable, de façon à éviter d'être requalifiés comme responsables du traitement.

Exemple de qualification de sous-traitant et de responsable du traitement (Source : RGPD. Guide du sous-traitant, CNIL, septembre 2017.)

Une entreprise A offre un service d'envoi de courriers de prospection commerciale en utilisant les fichiers clients d'autres entreprises B et C.

L'entreprise A est un sous-traitant des entreprises B et C dans la mesure où elle traite les données clients nécessaires à l'envoi des courriers pour le compte et sur les instructions des entreprises B et C.

Les entreprises B et C sont responsables du traitement de gestion de leurs clients, incluant l'envoi de courriers de prospection commerciale.

L'entreprise A est par ailleurs responsable du traitement s'agissant de la gestion du personnel dont elle est l'employeur, et de la gestion de ses clients, dont font partie les entreprises B et C.

Comment s'organisent les relations entre le responsable du traitement et son sous-traitant ?

Quand il décide de faire appel à un sous-traitant pour mettre en œuvre un traitement, le responsable du traitement doit respecter **deux obligations** :

- 1. Ne faire appel qu'à des sous-traitants présentant des garanties suffisantes** s'agissant de la mise en œuvre des mesures techniques et organisationnelles appropriées pour répondre aux exigences du RGPD et de la protection des droits des personnes concernées.

Le sous-traitant peut notamment justifier de l'existence de garanties suffisantes via l'application d'un code de conduite approuvé par la CNIL ou encore l'obtention d'une certification approuvée par cette autorité⁵.

Le responsable du traitement peut également, s'il en a la capacité, sélectionner son sous-traitant au moyen d'un cahier des charges ad hoc en matière de protection des données personnelles.

- 2. Contractualiser ses propres obligations et celles de son sous-traitant.** Cette contractualisation est réalisée sous forme écrite (acte juridique ou contrat), y compris au format électronique.

L'ORGANISATION CONTRACTUELLE DES RELATIONS ENTRE LES ACTEURS DU TRAITEMENT

Fiche
n° 4

ÉLÉMENTS À PRÉVOIR OBLIGATOIREMENT DANS LE CONTRAT AVEC LE SOUS-TRAITANT

Traitement des données par le sous-traitant **uniquement sur instruction documentée** du responsable du traitement

Obligation de confidentialité à la charge des personnes autorisées à traiter les données chez le sous-traitant (salariés, etc.)

Mise en place, par le sous-traitant, des **mesures techniques et organisationnelles aptes à assurer la sécurité des données** + aide du responsable du traitement à s'acquitter de ses propres obligations en la matière (analyses d'impact, mesures de sécurité, etc.)

Interdiction pour le sous-traitant de recruter un autre sous-traitant sans une autorisation écrite préalable, spécifique ou générale, du responsable du traitement (si autorisation générale, le responsable du traitement est informé sans délai et peut émettre des objections)

Obligation pour le sous-traitant de soumettre les sous-traitants ultérieurs aux mêmes obligations contractuelles que celles qui lui sont imposées par le contrat avec le responsable du traitement

Obligation pour le sous-traitant d'aider le responsable du traitement, dans la mesure du possible, à **donner suite aux demandes des personnes concernées** (par exemple : demandes d'accès, de rectification, de suppression, de portabilité, d'opposition)

Définition des modalités du traitement (objet, durée, nature et finalité du traitement, types de données et catégories de personnes concernées, obligations et droits du responsable du traitement)

Suppression ou restitution des données au responsable du traitement, par le sous-traitant, à l'issue du traitement (sauf disposition légale contraire)

Obligation, à la charge du sous-traitant, de **mettre à disposition du responsable du traitement les informations nécessaires à la preuve du respect de ses obligations et à la réalisation d'audits**



L'adhérent FFB faisant appel à un prestataire doit relire attentivement ses conditions générales de vente afin de vérifier que les éléments listés ci-dessus y figurent bien. Si ce n'est pas le cas, il faudra en demander l'ajout ou refuser de signer le contrat.



Pour les contrats déjà en cours, l'adhérent FFB devra réclamer à son prestataire la modification du contrat par voie d'avenant, de façon à rendre ce dernier conforme aux exigences du RGPD. Le prestataire ne peut pas refuser cette requête, car cela constituerait une faute susceptible de conduire à la résiliation du contrat.

L'ORGANISATION CONTRACTUELLE DES RELATIONS ENTRE LES ACTEURS DU TRAITEMENT

Fiche
n° 4

Qui est responsable de quoi ?

Le RGPD⁶ prévoit une répartition claire des responsabilités entre le responsable du traitement et le sous-traitant :

- ▶ Le responsable du traitement est responsable du dommage causé par la violation du RGPD.
- ▶ Le sous-traitant n'est responsable du dommage causé que s'il n'a pas respecté les obligations du RGPD lui incombant spécifiquement, en sa qualité de sous-traitant, ou s'il a agi en dehors des instructions licites du responsable du traitement.
- ▶ Le responsable du traitement ou le sous-traitant est exonéré de toute responsabilité s'il démontre que le fait ayant causé le dommage ne lui est nullement imputable.
- ▶ Le responsable du traitement ou le sous-traitant ayant acquitté intégralement la réparation du dommage peut se retourner contre les autres acteurs du traitement à hauteur de leur part de responsabilité.

À noter que, dans le cadre d'une action en réparation de son préjudice, toute personne concernée peut, en plus d'introduire une réclamation auprès de la CNIL⁷, engager indifféremment la responsabilité civile du responsable du traitement **ou** du sous-traitant. L'adhérent FFB prendra donc garde à vérifier que ce risque est suffisamment couvert par sa police d'assurance.

CONCLUSION

Quelles sont les étapes à suivre afin de se mettre en conformité ?

- 1. Identifier les traitements de données personnelles en cours au sein de la structure et les sous-traitants correspondants** (voir annexe de la **fiche n° 1** pour la liste des traitements les plus courants).
- 2. Utiliser les clauses contractuelles ou contrats types** (voir aussi modèles ci-après).
- 3. Contacter les sous-traitants actuels et leur demander, si nécessaire, une mise à jour des contrats déjà signés.**
- 4. Vérifier les CGV des prestataires proposant leurs services afin de s'assurer que les éléments obligatoires y figurent bien.**
- 5. Formaliser des procédures d'échanges et de remontées d'information afin de faciliter le respect des obligations respectivement imposées aux acteurs du traitement** (par exemple : demande d'aide pour la réalisation d'une analyse d'impact, réponse à la demande d'une personne concernée ou encore procédure à suivre en cas de violation des données personnelles).

MODÈLE DE CLAUSES CONTRACTUELLES

L'exemple de clauses de sous-traitance ci-dessous est celui proposé par la CNIL dans l'attente de l'adoption de clauses contractuelles types au sens du point 8 de l'article 28 du RGPD. Ces exemples de clauses peuvent être insérés dans les contrats des adhérents FFB. Elles doivent être adaptées et précisées selon la prestation de sous-traitance concernée. À noter qu'elles ne constituent pas, à elles seules, un contrat de sous-traitance.

Pour plus d'informations, consulter : « RGPD. Guide du sous-traitant » CNIL, septembre 2017⁸.

[...], situé à [...] et représenté par [...]

(ci-après, « le responsable du traitement »)

d'une part,

et

[...], situé à [...] et représenté par [...]

(ci-après, « le sous-traitant »)

d'autre part,

I. OBJET

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable du traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « **le règlement européen sur la protection des données** »).

II. DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE

Le sous-traitant est autorisé à traiter pour le compte du responsable du traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) [...].

La nature des opérations réalisées sur les données est [...].

La ou les finalité(s) du traitement sont [...].

Les données à caractère personnel traitées sont [...].

Les catégories de personnes concernées sont [...].

Pour l'exécution du service objet du présent contrat, le responsable du traitement met à la disposition du sous-traitant les informations nécessaires suivantes [...].

III. DURÉE DU CONTRAT

Le présent contrat entre en vigueur à compter du [...] pour une durée de [...].

IV. OBLIGATIONS DU SOUS-TRAITANT VIS-À-VIS DU RESPONSABLE DU TRAITEMENT

Le sous-traitant s'engage à :

1. Traiter les données **uniquement pour la ou les seules finalités** qui font l'objet de la sous-traitance.
2. Traiter les données **conformément aux instructions documentées** du responsable du traitement figurant en annexe du présent contrat. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection des données, il en **informe immédiatement** le responsable du traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.
3. Garantir **la confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat.
4. Veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :
 - ▶ s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;
 - ▶ reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
5. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception et de protection des données par défaut**.

6. Sous-traitance.

Choisir l'une des deux options

Option A (autorisation générale)

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « **le sous-traitant ultérieur** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable du traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable du traitement dispose d'un délai minimal de [...] à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable du traitement n'a pas émis d'objection pendant le délai convenu.

Option B (autorisation spécifique)

Le sous-traitant est autorisé à faire appel à l'entité [...] (ci-après, le « **sous-traitant ultérieur** ») pour mener les activités de traitement suivantes : [...]

En cas de recrutement d'autres sous-traitants ultérieurs, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique du responsable du traitement.

Quelle que soit l'option (autorisation générale ou spécifique)

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable du traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles

- ▶▶ appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations.

7. Droit d'information des personnes concernées

Choisir l'une des deux options

Option A

Il appartient au responsable du traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Option B

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doivent être convenus avec le responsable du traitement avant la collecte de données.

8. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable du traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Choisir l'une des deux options

Option A

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à [...] (indiquer un contact au sein du responsable du traitement).

Option B

Le sous-traitant doit répondre, au nom et pour le compte du responsable du traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

9. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans un délai maximum de [...] heures après en avoir pris connaissance et par le moyen suivant [...]. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable du traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Option possible

Après accord du responsable du traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable du traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, soixante-douze heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- ▶ La description de la nature de la violation de données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés.



- ▶ Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues.
- ▶ La description des conséquences probables de la violation de données à caractère personnel.
- ▶ La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable du traitement, le sous-traitant communique, au nom et pour le compte du responsable du traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- ▶ La description de la nature de la violation de données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés.
- ▶ Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues.
- ▶ La description des conséquences probables de la violation de données à caractère personnel.
- ▶ La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

10. Aide du sous-traitant dans le cadre du respect par le responsable du traitement de ses obligations

Le sous-traitant aide le responsable du traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable du traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

[Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres :

- ▶ La pseudonymisation et le chiffrement des données à caractère personnel;
- ▶ Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
- ▶ Les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- ▶ Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.]

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues par [code de conduite, certification].

[Dans la mesure où l'article 32 du règlement européen sur la protection des données prévoit que la mise en œuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en œuvre.]

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :

Au choix des parties

- ▶ Détruire toutes les données à caractère personnel.
- ▶ Ou renvoyer toutes les données à caractère personnel au responsable du traitement.
- ▶ Ou encore renvoyer les données à caractère personnel au sous-traitant désigné par le responsable du traitement.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois qu'elles sont détruites, le sous-traitant doit justifier par écrit de la destruction.

13. Délégué à la protection des données

Le sous-traitant communique au responsable du traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

14. Registre des catégories d'activités de traitement.

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement comprenant :

- ▶ Le nom et les coordonnées du responsable du traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données.
- ▶ Les catégories de traitements effectués pour le compte du responsable du traitement.
- ▶ Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale, et dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées.
- ▶ Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris, entre autres, selon les besoins :
 - ▶ la pseudonymisation et le chiffrement des données à caractère personnel ;
 - ▶ des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - ▶ des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
 - ▶ une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15. Documentation

Le sous-traitant met à la disposition du responsable du traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

V. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT VIS-À-VIS DU SOUS-TRAITANT

Le responsable du traitement s'engage à :

1. Fournir au sous-traitant les données visées au II des présentes clauses.
2. Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant.
3. Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant.
4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

1. Articles 4 et 24 du RGPD.

2. Article 26 du RGPD.

3. Articles 4 et 28 du RGPD.

4. Son rôle et ses obligations sont fixés à l'article 28 du RGPD.

5. Voir notamment les labels CNIL : <https://www.cnil.fr/fr/les-labels-cnil>.

6. Article 82 du RGPD.

7. Article 77 du RGPD.

8. https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf.