Règlement européen sur la protection des données personnelles

GUIDE DU SOUS-TRAITANT

EDITION SEPTEMBRE 2017

Applicable à partir du 25 mai 2018 à l'ensemble de l'Union européenne, le règlement européen sur la protection des données (RGPD) renforce les droits des résidents européens sur leurs données et responsabilise l'ensemble des acteurs traitant ces données (responsables de traitement et sous-traitants) qu'ils soient ou non établis au sein de l'Union européenne.

Le règlement impose des obligations spécifiques aux sous-traitants dont la responsabilité est susceptible d'être engagée en cas de manquement.

Ce guide a pour objectif de vous accompagner, en tant que sous-traitant, dans la mise en œuvre de ces nouvelles obligations.

Il pourra être enrichi de toutes les bonnes pratiques remontées par les professionnels.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Êtes-vous un sous-traitant au sens du règlement européen sur la protection des données ?

Vous êtes un sous-traitant si vous traitez des données personnelles pour le compte, sur instruction et sous l'autorité d'un responsable de traitement.

Pour rappel, **le responsable de traitement** est celui « *qui détermine les finalités et les moyens d'un traitement* » (article 4 du règlement européen – définitions).

Une **très grande variété de prestataires de services a la qualité de sous-traitant** au sens juridique du terme. Les activités des sous-traitants peuvent concerner une tâche bien précise (sous-traitance d'envoi de courriers) ou être plus générales et étendues (gestion de l'ensemble d'un service pour le compte d'un autre organisme telle que la gestion de la paie des salariés ou des agents par exemple).

Sont notamment concernés par le règlement européen :

- les prestataires de services informatiques (hébergement, maintenance,...), les intégrateurs de logiciels, les sociétés de sécurité informatique, les entreprises de service du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données,
- les agences de marketing ou de communication qui traitent des données personnelles pour le compte de clients et
- plus généralement, tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme.
- Un organisme public ou une association peut également être amené à recevoir une telle qualification.

Ne sont pas concernés, dans la mesure où ils n'ont pas accès et ne traitent pas de données à caractère personnel, les éditeurs de logiciels ou les fabricants de matériels (badgeuse, matériel biométrique, matériel médical).

A noter :

- Un organisme qui est sous-traitant est généralement responsable de traitement pour les traitements qu'il réalise pour son propre compte, et non pour ses clients (gestion de son personnel par exemple).
- Lorsqu'un organisme détermine la finalité et les moyens d'un traitement, il ne peut pas être qualifié de sous-traitant : un tel organisme doit être considéré comme étant un responsable de ce traitement (article 28.10 du règlement européen).

Exemple de qualification de sous-traitant et de responsable de traitement

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 de 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.

Outil : pour déterminer si vous êtes sous-traitant ou responsable de traitement, voir l'avis 1/2010 du groupe des CNIL européennes (G29) du 16 février 2010 qui précise le faisceau d'indices à utiliser dans le cadre d'une **analyse au cas par cas** :

- niveau d'instruction donné par le client au prestataire : quelle est l'autonomie du prestataire dans la réalisation de sa prestation ?
- degré de contrôle de l'exécution de la prestation : quel est le degré de « surveillance » du client sur la prestation ?
- valeur ajoutée fournie par le prestataire : le prestataire dispose-t-il d'une expertise approfondie dans le domaine ?
- degré de transparence sur le recours à un prestataire : l'identité du prestataire est-elle connue des personnes concernées qui utilisent les services du client ?

Texte officiel

Article 4 du règlement européen pour les définitions du responsable du traitement et du sous-traitant

Article 28.10 du règlement européen sur la notion de responsable du traitement

Êtes-vous soumis au règlement européen sur la protection des données ?

Vous entrez dans le champ du règlement européen en tant que sous-traitant :

- **si vous êtes établi dans l'UE** ou ;
- **lorsque vous n'êtes pas établi dans l'UE**, si :

  vos « *activités de traitement sont liées*

  - *à l'offre de biens ou de services à des personnes concernées dans l'UE ;*
  - *ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* » (article 3 du règlement européen).

Texte officiel

Article 3 du règlement européen sur le champ d'application territorial

Quel est le principal changement apporté par le règlement européen pour les sous-traitants ?

Aujourd'hui :

Les obligations de la loi Informatique et Libertés **ne s'imposent qu'au responsable de traitement**. En effet, en cas de recours à un sous-traitant :

- le **contrat** entre ce sous-traitant et le responsable du traitement doit indiquer les **obligations incombant au sous-traitant pour protéger la sécurité et la confidentialité des données** et prévoir qu'il ne peut agir que sur instruction du responsable du traitement ;
- ce sous-traitant doit présenter des **garanties suffisantes** pour assurer la mise en œuvre des mesures de sécurité et de confidentialité prévues à l'article 34 de la loi Informatique et Libertés ;
- cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

A partir du 25 mai 2018 :

Le règlement européen consacre une logique de **responsabilisation de tous les acteurs impliqués dans le traitement des données personnelles, dès lors qu'elles concernent des résidents européens**, que ces acteurs soient ou non établis au sein de l'UE[1].

Il impose **des obligations spécifiques aux sous-traitants** qui doivent notamment aider les responsables de traitement dans leur démarche permanente de mise en conformité de leurs traitements.

Texte officiel

Articles 28, 30.2 et 37 du règlement européen sur les obligations du sous-traitant

[1] Le considérant 13 du règlement européen rappelle en effet que l'adoption d'un « *règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques (…), pour offrir aux personnes physiques dans tous les Etats membres* ***un même niveau de droits opposables et d'obligations et de responsabilités pour les responsables du traitement et les sous-traitants*** ».

Quelles sont vos obligations à compter du 25 mai 2018 ?

Lorsque vous intervenez en tant que sous-traitant dans la mise en œuvre d'un traitement de données personnelles, vous devez offrir à votre client « ***des 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 présent règlement et garantisse la protection des droits de la personne concernée*** » (article 28 du règlement européen).

Vous devez notamment assister et conseiller votre client dans sa conformité à certaines obligations prévues par le règlement européen (analyses d'impact, notification de violation, sécurité, destruction des données, contribution aux audits).

Concrètement, cela implique :

1. Une obligation de transparence et de traçabilité

Vous devez :

- Etablir avec votre client un **contrat** ou un autre acte juridique précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du règlement européen.
- Recenser par écrit les instructions de votre client concernant les traitements de ses données afin de prouver que vous agissez « *sur instruction documentée du responsable de traitement* ».
- Demander l'autorisation écrite de votre client si, en tant que sous-traitant, vous faites vous-même appel à un sous-traitant.
- Mettre à la disposition de votre client **toutes les informations nécessaires pour démontrer le respect de vos obligations** et pour permettre la réalisation d'audits (sur la base, par exemple, du référentiel de la CNIL pour la délivrance de labels en matière de procédure d'audit).
- Tenir un **registre** qui recense vos clients et décrit les traitements que vous effectuez pour leur compte.

2. La prise en compte des principes de protection des données dès la conception et de protection des données par défaut

- Vous devez offrir à vos clients les **garanties nécessaires** afin que le traitement que vous mettez en œuvre pour leur compte réponde aux exigences du règlement européen et protège les droits des personnes concernées. Cela signifie notamment que :
    - **dès leur conception**, vos outils, produits, applications ou services que vous offrez à vos clients, intègrent de façon effective les principes relatifs à la protection des données et
    - **par défaut**, vos outils, produits, applications ou services garantissent que seules sont traitées les données nécessaires à la finalité du traitement au regard de la quantité de données collectées, de l'étendue de leur traitement, de la durée de conservation et du nombre de personnes qui y a accès.
- **A titre d'exemple**, ces principes peuvent impliquer :
    - de permettre à votre client de paramétrer par défaut et *a minima* la collecte de données et ne pas rendre techniquement obligatoire le renseignement d'un champ facultatif
    - de ne collecter que les données strictement nécessaires à la finalité du traitement (minimisation des données)

- de purger automatiquement et sélectivement les données d'une base active à l'issue d'une certaine durée ou
- de gérer des habilitations et droits d'accès informatiques « donnée par donnée » ou sur demande des personnes concernées (pour les réseaux sociaux par exemple).

3. Une obligation de garantir la sécurité des données traitées

- Vos employés qui traitent les données de vos clients doivent être soumis à une obligation de confidentialité.
- Vous devez notifier à votre client toute violation de ses données.
- Vous devez prendre toute mesure pour garantir un niveau de sécurité adapté aux risques.
- Au terme de votre prestation et selon les instructions de votre client, vous devez :
  - supprimer toutes les données ou les renvoyer à votre client
  - détruire les copies existantes sauf obligation légale de les conserver.

4. Une obligation d'assistance, d'alerte et de conseil

- Si, selon vous, une instruction de votre client constitue une **violation** des règles en matière de protection des données, **vous devez l'en informer immédiatement**.
- Lorsqu'une personne exerce ses droits (accès, rectification, effacement, portabilité, opposition, ne pas faire l'objet d'une décision individuelle automatisée, y compris le profilage) vous devez, **dans toute la mesure du possible**, **aider votre client** à donner suite à cette demande.
- Compte tenu des informations à votre disposition, **vous devez aider votre client** à garantir le respect des obligations en matière de sécurité du traitement, de notification de violation de données et d'analyse d'impact relative à la protection des données.

Par où commencer ?

1. Vérifiez si vous devez désigner un délégué à la protection des données

Le délégué à la protection des données est chargé de piloter la conformité au règlement européen au sein de l'organisme qui l'a désigné.

En tant que sous-traitant, vous devrez obligatoirement désigner un délégué à la protection des données en 2018 :

- Si vous êtes une autorité ou un organisme public ou
- Si vos activités de base vous amènent à réaliser, pour le compte de vos clients, un suivi régulier et systématique des personnes à grande échelle ou
- Si vos activités de base vous amènent, pour le compte de vos clients, à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Au-delà de ces cas obligatoires, la désignation d'un délégué à la protection des données est recommandée car elle permet de disposer d'un expert chargé de la mise en œuvre concrète et du pilotage de la conformité au règlement européen.

Exemples

Les lignes directrices du G29 sur le délégué à la protection des données adoptées le 5 avril 2017 donnent deux exemples de **désignation obligatoire d'un délégué par un sous-traitant** :

Exemple n° 1 : une petite entreprise familiale active dans le secteur de la distribution d'appareils électroménagers dans une seule ville recourt aux services d'un sous-traitant dont l'activité de base consiste à fournir des services d'analyse de sites internet et d'assistance à la publicité et au marketing ciblés. Les activités de l'entreprise familiale et ses clients n'entraînent pas de traitement de données à «grande échelle», compte tenu du faible nombre de clients et des activités relativement limitées. Toutefois, prises globalement, les activités du sous-traitant, qui dispose d'un grand nombre de clients comme cette petite entreprise, consistent en un traitement à grande échelle. Le sous-traitant doit donc désigner un délégué en vertu de l'article 37, paragraphe 1, point b) du règlement européen. L'entreprise familiale n'est quant à elle pas soumise à l'obligation de désigner un délégué.

Exemple n° 2 : une entreprise de taille moyenne spécialisée dans la fabrication de carrelage sous-traite ses services de médecine du travail à un sous-traitant externe, qui dispose d'un grand nombre de clients similaires dans le département du Tarn. Le sous-traitant doit désigner un délégué en vertu de l'article 37, paragraphe 1, point c), dans la mesure où le traitement s'effectue à grande échelle. En revanche, le fabricant n'est pas nécessairement tenu de désigner un délégué.

Le délégué désigné par un sous-traitant supervise également les activités menées par l'organisation sous-traitante lorsqu'elle agit elle-même en qualité de responsable du traitement des données (par exemple ressources humaines, informatique, logistique).

Pour approfondir :

Consultez la page dédiée sur le site de la CNIL

Texte officiel

Article 37 du règlement européen sur la désignation obligatoire d'un délégué à la protection des données par un sous-traitant

2. Analysez et révisez vos contrats

Ce contrat doit définir :

- l'objet et la durée de la prestation que vous effectuez pour le compte de votre client
- la nature et la finalité du traitement

- le type de données à caractère personnel que vous traitez pour le compte de votre client
- les catégories de personnes concernées
- les obligations et les droits de votre client en tant que responsable de traitement
- vos obligations et vos droits en tant que sous-traitant tels que prévus à l'article 28 du règlement

Exemple de clause

Le présent guide propose un exemple de clauses de sous-traitance dans l'attente de l'adoption de clauses contractuelles types au sens de l'article 28.8 du règlement européen. Ces exemples de clauses peuvent être insérés dans vos contrats. Elles doivent adaptées et précisées selon la prestation de sous-traitance concernée. A noter qu'elles ne constituent pas, à elles seules, un contrat de sous-traitance.

Texte officiel

Considérant 81 et article 28 du règlement européen sur les obligations du sous-traitant

3. Elaborez un registre des traitements

En tant que sous-traitant, vous devez tenir un **registre des catégories d'activités de traitement** que vous effectuez pour le compte de vos clients.

Ce registre doit être tenu par écrit et contenir :

- le nom et les coordonnées de chaque client pour le compte duquel vous traitez des données
- le nom et les coordonnées de chaque sous-traitant ultérieur, le cas échéant
- le nom et les coordonnées du délégué à la protection des données, le cas échéant
- les catégories de traitements effectués pour le compte de chaque client
- les transferts de données hors UE que vous effectuez pour le compte de vos clients, le cas échéant
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en place.

A noter

Vous avez par ailleurs la qualité de responsable de traitement pour les opérations que vous mettez en œuvre sur vos propres données (par exemple pour la gestion de votre personnel ou la gestion de vos clients). Dès lors, **deux registres sont à tenir** : un pour les traitements dont vous êtes responsable et un autre pour les traitements que vous opérez, en tant que sous-traitant, pour le compte de vos clients.

Modèle de registre

Un modèle de registre est proposé à l'étape 2 : cartographier vos traitements du guide en ligne 6 étapes pour se préparer au règlement européen

Texte officiel

Article 30.2 du règlement européen sur la tenue du registre par un sous-traitant

Article 30.1 du règlement européen pour la tenue du registre par un responsable de traitement

Si je fais appel à un autre sous-traitant, quelles sont mes obligations ?

En tant que sous-traitant, vous ne pouvez recruter un autre sous-traitant qu'après avoir obtenu **l'autorisation écrite de votre client**. Cette autorisation peut être, au choix des parties :

- **spécifique**, c'est-à-dire accordée pour un sous-traitant particulier ou
- **générale**, vous devrez informer votre client de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants, permettant ainsi à votre client d'émettre des objections sur ces changements.

Le sous-traitant que vous recrutez est soumis aux **mêmes obligations que celles prévues dans votre contrat avec votre client responsable de traitement**. Il doit en particulier présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour que le traitement soit conforme au règlement européen.

Attention !

Si le sous-traitant que vous recrutez ne respecte pas ses obligations, vous êtes **pleinement responsable** vis-à-vis du responsable de traitement de l'exécution par ce sous-traitant de ses obligations.

Texte officiel

Articles 28.2 et 28.4 du règlement européen sur le recrutement d'un sous-traitant par un sous-traitant

Les contrats en cours avec mes clients doivent-ils être modifiés ?

Oui, tous les contrats de sous-traitance en cours d'exécution devront comprendre au 25 mai 2018 les clauses obligatoires prévues par le règlement européen.

Il est donc recommandé à tous les sous-traitants :

- d'anticiper cette évolution du cadre juridique applicable **en intégrant dès à présent et par avenant les clauses dans les contrats en cours avec leurs clients, tout en prévoyant qu'elles ne seront opposables qu'à compter du 25 mai 2018**
- de procéder dès cette date à **des vérifications et/ou audits** vous permettant de vous assurer du respect de vos obligations en tant que sous-traitant et de réaliser les ajustements nécessaires.

Exemple de clauses

Le présent guide propose un exemple de clauses de sous-traitance dans l'attente de l'adoption de clauses contractuelles types au sens de l'article 28.8 du règlement européen. Ces exemples de clauses peuvent être insérés dans vos contrats. Elles doivent adaptées et précisées selon la prestation de sous-traitance concernée. A noter qu'elles ne constituent pas, à elles seules, un contrat de sous-traitance.

Quel est mon rôle en cas de violation de données ?

Une **violation de données** est une faille de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à ces données.

Vous devez notifier à votre client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Sur la base de cette notification, votre client, en tant que **responsable de traitement**, devra quant à lui notifier cette violation de données **à l'autorité de contrôle compétente** dans les conditions de l'article 33 du règlement européen et communiquer à la personne concernée une telle violation dans les conditions de l'article 34 du règlement européen.

Sous réserve de l'accord de votre client et à condition que cela soit prévu explicitement par le contrat vous liant avec votre client, il est possible pour ce dernier de vous donner instruction d'effectuer **pour son compte** cette notification à l'autorité et, le cas échéant aux personnes concernées (voir les exemples de clauses à la fin du présent guide).

Texte officiel :

Articles 4.12, 33 et 34 du règlement européen

Quel est mon rôle dans le cadre de l'analyse d'impact ?

Votre client, en tant que **responsable de traitement**, doit réaliser une analyse d'impact des traitements envisagés sur la protection des données dans les conditions prévues à l'article 35 du règlement européen. La réalisation d'une telle analyse ne relève donc pas de votre responsabilité.

Toutefois, vous devez **aider votre client dans la réalisation de cette analyse et lui fournir toute l'information nécessaire**. Cette assistance doit être prévue dans votre contrat avec votre client.

Texte officiel :

Article 28.3 f) du règlement européen et lignes directrices du G29 relatives à l'analyse d'impact (p.13)

Puis-je bénéficier du mécanisme de guichet unique ?

Si vous êtes établis dans plusieurs États membres de l'UE, vous pouvez bénéficier du mécanisme de guichet unique.

Il permet aux organismes qui mettent en œuvre des traitements transfrontaliers (établissements dans plusieurs Etats membres ou traitements affectant des personnes dans plusieurs Etats membres) de dialoguer avec une seule autorité de contrôle nationale qui prendra des décisions applicables à l'ensemble des Etats membres concernés par ces traitements. Cette autorité est appelée « *autorité chef de file* ».

Votre autorité chef de file sera celle de **votre établissement principal**, c'est-à-dire du lieu de votre administration centrale dans l'UE. Si vous ne disposez pas d'administration centrale dans l'UE, il s'agira alors de l'établissement dans l'UE où se déroule l'essentiel de vos activités de traitement.

Texte officiel

Articles 4.16, 56 et considérant 36 du règlement européen et lignes directrices du G29 relatives à la désignation d'une autorité chef de file (p. 9)

Quelles sont mes obligations si je ne suis pas établi dans l'UE ?

Si vous ne disposez pas d'établissement dans l'UE, vous êtes soumis à l'ensemble des dispositions du règlement européen dès lors :

- que vous procédez, pour le compte de votre client, à des traitements de données de personnes se trouvant dans l'UE
- que vous offrez, pour le compte de votre client, des biens ou des services ou suivez le comportement de ces personnes.

Vous devez alors **désigner un représentant** dans l'UE pour être **l'interlocuteur des personnes concernées et des autorités de contrôle** pour toute question relative à ces traitements.

Texte officiel :

Articles 3 et 27 du règlement européen

Quels sont les risques en cas de non-respect de mes obligations ?

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement européen peut obtenir la **réparation intégrale de son préjudice de la part du responsable de traitement ou du sous-traitant**.

Vous pouvez donc être tenu pour **responsable du dommage causé** et faire l'objet de **sanctions administratives importantes** pouvant s'élever, selon la catégorie de l'infraction, jusqu'à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, jusqu'à 2% ou 4% du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu. Ces sanctions peuvent s'appliquer par exemple dans les cas suivants :

- si vous agissez en dehors des instructions licites de votre client ou contrairement à ces instructions ;
- si vous n'aidez pas votre client à respecter ses obligations (notamment notification d'une violation de données ou réalisation d'une analyse d'impact) ;
- si vous ne mettez pas à la disposition de votre client les informations permettant de démontrer le respect des obligations ou pour permettre la réalisation d'audits ;
- si vous n'informez pas votre client qu'une instruction constituerait une violation du règlement européen ;
- si vous sous-traitez sans autorisation préalable de votre client ;
- si vous faites appel à un sous-traitant qui ne présente pas de garanties suffisantes ;
- si vous ne désignez pas un délégué à la protection des données lorsque cela est obligatoire ou encore
- si vous ne tenez pas de registre des catégories d'activités de traitement que vous mettez en œuvre pour le compte de vos clients.

Texte officiel :

Articles 82 et 83 du règlement européen

Exemple de clauses contractuelles de sous-traitance

L'exemple de clauses de sous-traitance ci-dessous est proposé dans l'attente de l'adoption de clauses contractuelles types au sens de l'article 28.8 du règlement européen. Ces exemples de clauses peuvent être insérés dans vos contrats. Elles doivent adaptées et précisées selon la prestation de sous-traitance concernée. A noter qu'elles ne constituent pas, à elles seules, un contrat de sous-traitance.

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

(ci-après, « ***le responsable de 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 de 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 de 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 de 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 de traitement

Le sous-traitant s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance
2. traiter les données **conformément aux instructions documentées** du responsable de 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 Etats membres relative à la protection des données, il en **informe immédiatement** le responsable de 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 de 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 de traitement dispose d'un délai minium 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 de 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 de 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 de 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 de 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 de 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 doit être convenue avec le responsable de traitement avant la collecte de données.

8. **Exercice des droits des personnes**

Dans la mesure du possible, le sous-traitant doit aider le responsable de 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 de traitement*).

Option B

Le sous-traitant doit répondre, au nom et pour le compte du responsable de 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 de 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 de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Option possible

Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 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 de traitement, le sous-traitant communique, au nom et pour le compte du responsable de 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 de traitement de ses obligations

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

Le sous-traitant aide le responsable de 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
- à renvoyer toutes les données à caractère personnel au responsable de traitement ou
- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

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

13. **Délégué à la protection des données**

Le sous-traitant communique au responsable de 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 de traitement comprenant :

- le nom et les coordonnées du responsable de 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 de 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 de traitement vis-à-vis du sous-traitant

Le responsable de 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