MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

DÉLÉGUÉ MINISTÉRIEL à la PROTECTION des DONNÉES

Annexe III : Clauses contractuelles « RGPD » du ministère de l'intérieur

Sommaire

Introduction 3

Clauses contractuelles du ministère de l'intérieur relatives à la sous-traitance de données personnelles 4

Définitions spécifiques aux données à caractère personnel 4

SECTION I 4

Clause 1 Objet et champ d'application 5

Clause 2 Invariabilité des clauses 5

Clause 3 Interprétation 5

Clause 4 Hiérarchie 5

SECTION II 5

OBLIGATIONS DES PARTIES 5

Clause 6 Description du ou des traitements 6

Clause 7 Obligations des parties 6

7.1. Instructions 6

7.2. Limitation de la finalité 6

7.3. Durée du traitement des données à caractère personnel 6

7.4. Sécurité du traitement 6

7.5. Données sensibles 7

7.6. Documentation et conformité 7

7.7. Recours à des sous-traitants ultérieurs 8

7.8. Transferts de données hors de l'Union européenne ou traitement par un prestataire soumis à un droit extraterritorial tiers 8

7.9 Sort des données 9

Clause 8 Assistance au responsable du traitement 9

Clause 9 Notification de violations de données à caractère personnel 10

SECTION III 11

DISPOSITIONS FINALES 11

Clause 10 Non-respect des clauses et résiliation 11

ANNEXE I 13

Liste des parties ..... **Erreur ! Signet non défini.**

ANNEXE II 14

Description du traitement 14

ANNEXE III 15

Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données 15

ANNEXE IV 16

Liste de sous-traitants ultérieurs 16

Introduction

Les clauses suivantes sont à utiliser lors du recours à un prestataire pour un traitement impliquant des données personnelles. Pour les aspects SSI de cette prestation, on se reportera aux *Clauses de sécurité types des marchés publics ou accords-cadres* (PGSN - E1) du SHFD.

Que les traitements soient basés sur le Règlement européen 2016/679 (RGPD) ou sur le titre III de la loi informatique et libertés, la signature d'un contrat ou d'une convention contenant des mentions obligatoires est requise (article 28 du RGPD ou, pour les traitements relevant de la directive police-justice, article 96 de la loi n°78-17 Informatique et libertés). Les clauses qui suivent sont utilisables dans les deux situations.

Il est rappelé que dans ce qui suit, on entend par « **sous-traitant** » l'entité publique ou privée qui traite des données personnelles pour le compte et sur les instructions du responsable du traitement.

Attention

Au sens du code de la commande publique, il s'agit du prestataire.

Celui que le CCP nomme « sous-traitant » sera, au sens du RGPD, un « sous-traitant ultérieur » ou « secondaire »).

Il est à noter que les services et les opérateurs du ministère peuvent être en position de responsables de traitement, ou bien être eux-mêmes des sous-traitants (DNUM, ST(SI)2, ANTS, ANSC…). En cas de marché passé par un acheteur public pour le compte d'un service client, c'est bien ce dernier qui est responsable du traitement.

La Commission européenne a adopté le 4 juin 2021 une décision d'exécution (UE) 2021/91 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28 du RGPD.

Les autorités européennes de protection des données ont émis début 2021 leur avis sur ces clauses (*Avis conjoint 1/2021 du comité européen de la protection des données et du Contrôleur européen de la protection des données*).

Afin de faciliter la rédaction des contrats et des conventions de sous-traitance pour les traitements du ministère et de ses opérateurs, les services pourront inclure dans leurs contrats ou conventions les clauses suivantes, inspirées des clauses types de la Commission et adaptées aux spécificités du ministère (activités régaliennes et de police). S'il n'est pas possible d'insérer ces clauses telles quelles (cas d'un marché interministériel, par exemple), on veillera à conserver des dispositions équivalentes.

L'attention est attirée sur le fait qu'il ne suffit pas de recopier ces clauses dans le contrat, mais qu'elles doivent être, à plusieurs endroits, précisées au cas par cas, et que les annexes doivent être remplies de manière spécifique pour chaque contrat.

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

DÉLÉGUÉ MINISTÉRIEL à la PROTECTION des DONNÉES

Clauses contractuelles du ministère de l'intérieur relatives à la sous-traitance de données personnelles

Ce document décrit les engagements réciproques entre le Service Militaire Adapté (Ministère des Outre-mer), ci-après appelé le Responsable de traitement, et le titulaire, ci-après appelée le Sous-traitant, concernant les données à caractère personnel qui ont vocation à être traitées par le Sous-traitant.

Les Parties reconnaissent que le Sous-traitant n'acquiert aucun droit sur les données traitées ou notamment exploitées, hébergées, sauvegardées ou encore stockées pour le compte du Responsable de traitement et à l'initiative de celui-ci, dans le cadre de la sous-traitance.

Dans le cas où le Responsable de traitement sous-traite plusieurs traitements à un même Sous-traitant, un document distinct est rempli et signé pour chaque traitement.

Définitions spécifiques aux données à caractère personnel

Donnée à caractère personnel : désigne toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro de téléphone, une adresse courriel, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Traitement : désigne toute opération ou tout ensemble d'opérations réalisé sur les données à caractère personnel, de manière automatisée ou non, tels que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, le verrouillage, l'effacement ou la destruction.

Instruction : désigne toute commande explicative écrite, reçue par le Sous-traitant de la part du Responsable de traitement en vertu du présent contrat et du document distinct rédigé pour chaque fichier contenant de données à caractère personnel.

Responsable de traitement : désigne 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 ; dans le cadre du présent contrat, le Responsable de traitement est le Service militaire adapté.

Sous-traitant : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles sur instruction pour le compte du Responsable du traitement.

Violation des données à caractère personnel : il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité des données personnelles.

Clausier

SECTION I

Clause 1 Objet et champ d'application

a) Les présentes clauses contractuelles types (ci-après les «clauses») ont pour objet de garantir la conformité avec , selon les cas, l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ou, pour les traitements relevant de la directive police-justice, l'article 96 de la loi n°78-17 Informatique et libertés.
b) Les responsables du traitement et les sous-traitants énumérés à l'annexe I ont accepté ces clauses afin de garantir le respect des dispositions précitées.
c) Les présentes clauses s'appliquent au traitement des données à caractère personnel tel que décrit à l'annexe II.
d) Les annexes I à IV font partie intégrante des clauses.
e) Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés.
f) Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés.

Clause 2 Invariabilité des clauses

a) Les parties s'engagent à ne pas modifier les clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent.
b) Les parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

Clause 3 Interprétation

a) Lorsque des termes définis dans le règlement (UE) 2016/679 figurent dans les clauses, ils s'entendent comme dans le règlement en question.
b) Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679 et de la loi Informatique et libertés respectivement.
c) Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 et/ou par la loi Informatique et libertés, ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

Clause 4 Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront, conformément à l'article 6.1 du CCAP, relatif à l'ordre de priorité des pièces contractuelles.

SECTION II

OBLIGATIONS DES PARTIES

Clause 6 Description du ou des traitements

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés à l'annexe II.

Clause 7 Obligations des parties

7.1. Instructions

a) Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.
   Les personnes habilitées à donner des instructions sont les représentants du SMA, les personnes habilitées à recevoir les instructions sont les représentant du titulaire. Tout moyen de communication permettant de déterminer de façon certaine la date et l'heure de réception peut être utilisé pour l'échange d'information, conformément à l'article 11.2 du CCAP.
b) Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

7.2. Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l'annexe II, sauf instruction complémentaire du responsable du traitement.

7.3. Durée du traitement des données à caractère personnel

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée à l'annexe II.

7.4. Sécurité du traitement

a) Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.
b) La modification des mesures techniques et organisationnelles déployées pour le Traitement doit être autorisée préalablement par le Responsable de traitement selon les modalités prévues à la

clause 7.1.a. Quelle que soit la modification apportée, le Sous-traitant doit garantir un niveau de sécurité au moins équivalent entre les nouvelles mesures et les anciennes mesures.

c) Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

7.5. Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires telles qu'exigées par le Responsable de traitement en annexe III.

Le cas échéant, le responsable de traitement informe le sous-traitant des obligations spécifiques engendrées par ce type de données (par exemple, données de santé nécessitant une certification HDS).

7.6. Documentation et conformité

a) Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.

b) Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.

c) Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.

d) Le responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.
Conformément à l'article 12 du CCAP, le titulaire est informé quinze jours à l'avance de la date de l'audit et des modalités.
L'administration, ou l'organisme mandaté à cette fin, peut, pendant une période de six mois à compter du terme de l'exécution de l'accord-cadre ou de sa résiliation, exercer un contrôle dans les locaux du titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées.

e) Les parties mettent à la disposition de l'autorité de contrôle compétente, dès que celle-ci en fait la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

f) Le Sous-traitant doit être en mesure de fournir au Responsable de traitement à tout moment une liste des personnes autorisées à accéder aux données.

Le Sous-traitant doit communiquer sur demande la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.).

7.7. Recours à des sous-traitants ultérieurs

a) Le sous-traitant n'est pas autorisé à sous-traiter à un sous-traitant ultérieur les opérations de traitement qu'il effectue pour le compte du responsable du traitement en vertu des présentes clauses sans l'autorisation écrite spécifique préalable du responsable du traitement (la demande se fait via le formulaire DC4). Le sous-traitant soumet la demande d'autorisation spécifique au moins quatre semaines avant le recrutement du sous-traitant ultérieur en question, ainsi que les informations nécessaires pour permettre au responsable du traitement de prendre une décision au sujet de l'autorisation. La liste des sous-traitants ultérieurs autorisés par le responsable du traitement figure à l'annexe IV, que les parties tiennent à jour.

b) Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés.

c) À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.

d) Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

e) Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

7.8. Transferts de données hors de l'Union européenne ou traitement par un prestataire soumis à un droit extraterritorial tiers

N.B. : ce paragraphe ne vaut que pour les traitements relevant du RGPD. La directive police-justice et le titre III de la loi Informatique et libertés ne permettent pas le transfert de données vers un sous-traitant hors de l'Union européenne.

Le Sous-traitant s'engage à informer le Responsable de traitement de la localisation physique des serveurs hébergeant les Données à caractère personnel.

a) Si le sous-traitant est localisé hors de l'Union européenne, ou s'il est localisé dans l'Union, mais soumis à un droit extraterritorial tiers, il doit préalablement fournir au Responsable du traitement les garanties exigées par l'article 46 du règlement (UE) 2016/679 pour validation par le délégué ministériel à la protection des données.

b) Le Sous-traitant doit fournir au Responsable de traitement une liste des pays destinataires mise à jour. En cas de modification des pays destinataires par le Sous-traitant, ce dernier doit en informer préalablement le Responsable de traitement.

c) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant, ou tout traitement par un prestataire soumis à un droit extraterritorial tiers, n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou à la loi Informatique et libertés. Dans ce cas, le Sous-traitant informe le Responsable de traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

d) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, ou que ce sous-traitant ultérieur est soumis à un droit extraterritorial tiers, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 ou de la loi Informatique et libertés en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'article 46, paragraphe 2, du règlement (UE) 2016/679, **pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies et que les garanties exigées par le RGPD et par la loi Informatique et libertés lui soient préalablement soumises pour validation par le délégué ministériel à la protection des données.**

7.9 Sort des données

Le Sous-traitant s'engage, dans un délai d'un (1) mois calendaire avant la date de fin de contrat, à interroger le Responsable de traitement sur le sort des données traitées. Au choix du Responsable de traitement, le Sous-traitant s'engage à :

- détruire toutes les Données à caractère personnel ;
- renvoyer toutes les Données à caractère personnel au Responsable de traitement sous un format exploitable à préciser. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Sous-traitant. Une fois les Données détruites, le Sous-traitant doit justifier par écrit de la destruction ;
- renvoyer toutes 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 les Données détruites, le Sous-traitant doit justifier par écrit de la destruction.

Clause 8 Assistance au responsable du traitement

a) Le sous-traitant transmet sans délai au responsable du traitement toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande.

b) Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits. Dans l'exécution de ses obligations conformément aux points a) et b), le sous-traitant se conforme aux instructions du responsable du traitement.

c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu des informations dont dispose le sous-traitant:

1) l'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel («analyse d'impact relative à la protection des données») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques;
2) l'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque;
3) l'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes;
4) les obligations prévues à l'article 32 du règlement (UE) 2016/679.

d) L'annexe III précise les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

Clause 9 Notification de violations de données à caractère personnel

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679 ou des articles de la loi Informatique et libertés.

9.1. Violation de données en rapport avec des données traitées par le responsable du traitement

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement :

a) aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente, éventuellement décidée et effectuée par le responsable de traitement, dans les meilleurs délais après que le responsable du traitement en a eu connaissance ;
b) aux fins de l'obtention des informations suivantes qui doivent inclure, au moins:

1) la nature des 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;
2) les conséquences probables de la violation de données à caractère personnel;
3) les mesures prises ou les mesures 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.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, le sous-traitant fournit les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

9.2. Violation de données en rapport avec des données traitées par le sous-traitant

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe le responsable du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

a) une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés);
b) les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel;
c) ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

La décision de notifier ou pas cette violation à l'autorité de protection des données, ainsi qu'aux personnes concernées, et la forme de la communication éventuelle, relèvent du responsable de traitement uniquement. Sauf instruction contraire, c'est lui qui procède à ces notifications et à la communication.

Les parties définissent à l'annexe III tous les autres éléments que le sous-traitant doit communiquer lorsqu'il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en application des articles 33 et 34 du règlement (UE) 2016/679 ou de la loi Informatique et libertés.

SECTION III

DISPOSITIONS FINALES

Clause 10 Non-respect des clauses et résiliation

a) Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.
   Le responsable peut également enjoindre au sous-traitant de se mettre en conformité sous astreinte, dans un délai qu'il fixera. L'astreinte pourra atteindre 350€ par jour de retard.
b) Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :

   1) le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au point a) et le respect des présentes clauses n'est pas

rétabli dans un délai raisonnable indiqué par le responsable de traitement dans son injonction de mise en conformité et, en tout état de cause, dans un délai d'un mois à compter de la suspension;

2) le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés;

3) le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés.

c) Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.

d) À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

ANNEXE I

L'annexe I fait l'objet d'un document séparé.

ANNEXE II

Description du traitement

Catégories de personnes concernées dont les données à caractère personnel sont traitées

Les catégories de personnes concernées par le traitement des données à caractère personnel sont les agents en charge de l'exécution de l'accord-cadre, les volontaires stagiaires, les volontaires techniciens et les personnels d'encadrement du SMA.

Catégories de données à caractère personnel traitées

Les données à caractère personnel traitées sont les informations se rapportant à une personne physique identifiée ou identifiable. Ces données sont les suivantes : nom, prénom, date de naissance, lieu de naissance, numéro de sécurité sociale (qu'il soit temporaire ou définitif), numéros d'identifiant (de contrat, ou numéro d'identifiant défense), sexe, lieu de résidence, lieu de travail (stage, contrat en alternance, CDD, …), salaire, emploi du temps, motif d'absence. Chaque donnée est issue d'un justificatif qui fait l'objet d'une collecte et est conservé (photocopie de pièce d'identité, photocopie de carte vitale, contrat de travail, extrait d'acte de naissance, …). A ces données s'ajoutent toutes autres données nécessaires à la bonne exécution de l'accord-cadre.

Nature du traitement

La nature des opérations réalisées sur les données est la collecte, la consultation, la modification, l'export, le traitement et la conservation.

Finalité(s) pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du responsable du traitement

La ou les finalité(s) du traitement sont multiples pour le fonctionnement de l'état-major et des régiments du Service militaire adapté tels que la conservation et la production des données auprès d'institutions françaises et/ou européennes.

Durée du traitement

La durée du traitement correspond à la durée de l'accord-cadre.

ANNEXE III

Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données

Ces mesures viennent en complément de l'annexe au CCAP PSSI.

Le sous-traitant indique dans son offre tous les éléments permettant d'attester sa capacité à assurer la protection des données personnelles de l'accord-cadre (ex : certification ISO 27001 etc.).

Le titulaire devra a minima être en capacité de chiffrer les informations comportant des données à caractères personnelles avec des solutions de chiffrement qualifiées par l'ANSSI (Zone Central, Zed, …) ou ACID fourni gracieusement par le Ministère des armées aux industriels de la défense.

Le titulaire présente dans son offre les éléments techniques mis œuvre afin de garantir la sécurité des données.

ANNEXE IV

Liste de sous-traitants ultérieurs

NOTE EXPLICATIVE:

La présente annexe doit être complétée en cas d'autorisation spécifique de sous-traitants ultérieurs [clause 7.7, point a), option 1].

Le responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants:

1. Nom: …
   Adresse: …

Nom, fonction et coordonnées de la personne de contact: …
Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés): …

2.