Annexe relative au traitement des données à caractère personnel (RGPD)

Annexe 2 du CCAP



**L’État représenté par le** **Ministère de la Justice,** dont le siège est situé à Hôtel de Bourvallais, 13 place Vendôme, 75001 Paris, représenté par **Carine CHEVRIER, Secrétaire générale,** au nom et pour le compte de l’État,

(ci-après, « ***le responsable de traitement*** » ou « *le ministère »*)

d'une part,

**ET**

*[A compléter par le sous-traitant]*, société au capital de *[A compléter par le sous-traitant]* euros dont le siège social est situé à *[A compléter par le sous-traitant]*, inscrite au RCS de *[A compléter par le sous-traitant]* sous le numéro *[A compléter par le sous-traitant]*, représenté par *[A compléter par le sous-traitant]* agissant en qualité de *[A compléter par le sous-traitant]*,

(ci-après, ***« le sous-traitant »***)

d’autre part,

Ci-après collectivement désignés « ***les parties*** ».

1. **Définitions**

Les termes « données à caractère personnel », « traitement », « responsable de traitement » et « sous-traitant » sont définis conformément à l’article 4 du Règlement Général sur la Protection des Données.

1. **Objet**

La présente annexe est conclue en application de l’article VII.2 du CCAP de l’accord-cadre relatif à *[A compléter par le MINJUS avec nom de l’accord-cadre, n° de marché (long) et n° Chorus (court)]* dans le cadre d’une sous-traitance de traitement de données à caractère personnel.

Les présentes dispositions ont pour objet de définir les conditions dans lesquelles le sous-traitant s’engage à effectuer au nom et 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 dit Règlement Général sur la Protection des Données (ci-après le « RGPD»), la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 ainsi que la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi « Informatique et Libertés »).

Ainsi, la présente convention est conclue en application des dispositions du paragraphe 3 de l’article 28 du RGPD, et le cas échéant de l’article 96 de la loi « Informatique et Libertés », qui imposent de définir l’objet et la durée du traitement de données à caractère personnel, sa nature et sa finalité, le type de données à caractère personnel, les catégories de personnes concernées ainsi que les droits et les obligations du responsable de traitement.

Les appendices 1, 2 et 3 font partie intégrante de la présente annexe.

1. **Description du traitement faisant l’objet de la sous-traitance**

Le sous-traitant est autorisé à traiter au nom et pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir les services précisés dans les documents du marché.

Le détail 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’appendice 1.

1. **Durée du contrat**

Les présentes clauses entrent en vigueur à la date de leur signature par les parties et pour la durée de validité du marché.

Les présentes clauses sont renouvelables par tacite reconduction pour une durée identique, sauf dénonciation par l’une ou l’autre des parties, en respectant un préavis de six mois avant la date de renouvellement du contrat, par lettre recommandée avec demande d’avis de réception.

1. **Obligations du sous-traitant vis-à-vis du responsable de traitement**

Le sous-traitant s'engage à :

1. Traiter les données **uniquement pour les seules finalités** qui font l’objet de la sous-traitance.
2. Traiter les données **conformément aux instructions documentées** du responsable de traitement. 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 et 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. Edicter à son personnel des directives relatives à la mise en œuvre des mesures prévues par la réglementation nationale et européenne relative à la protection des données à caractère personnel et à la démonstration du respect de cette dernière. L’application par le sous-traitant de codes de conduite ou de mécanismes de certification approuvés, voire d’indications données par un délégué à la protection des données peut servir à démontrer le respect des obligations incombant au responsable de traitement.

Plus généralement, aucune donnée ne peut être utilisée, consultée, valorisée, modifiée et communiquée par le sous-traitant sans l'accord du responsable de traitement.

1. **Instructions**

Le sous-traitant est tenu de traiter les données à caractère personnel uniquement pour le compte du ministère et conformément aux instructions documentées de ce dernier.

Le ministère donnera ses instructions, préalablement à la mise en œuvre du traitement et par écrit, sauf si l’urgence ou d’autres circonstances nécessitent que les instructions soient données à l’oral. Dans ce cas, le ministère les confirmera par écrit dans un délai raisonnable.

Le ministère peut préciser et/ou compléter les instructions données et donner de nouvelles instructions.

Si le sous-traitant considère qu’une instruction constitue une violation du règlement général 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.

1. **Règles relatives à la sous-traitance ultérieure**

Définition : un sous-traitant ultérieur signifie tout autre sous-traitant, engagé par le sous-traitant initial pour la fourniture des services ou d’une partie des services pour le compte du ministère.

Le sous-traitant dispose de l’autorisation du responsable de traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d’une liste convenue en appendice 2.

Pour tout ajout ou modification au cours de la relation contractuelle, le sous-traitant soumet la demande d’autorisation au moins *[A compléter par le MINJUS/MOA : préciser la durée]* avant le recrutement du sous-traitant ultérieur en question, ainsi que les informations nécessaires pour permettre au responsable de traitement de prendre une décision au sujet de l’autorisation. La liste des sous-traitants ultérieurs autorisés par le responsable de traitement figure à l’appendice 2 que les parties tiennent à jour.

En tout état de cause, 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 de traitement en vertu des présentes clauses sans l’autorisation écrite, spécifique et préalable du responsable de traitement.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable de 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 du présent contrat, du RGPD et de la loi « Informatique et Libertés ».

En particulier, le sous-traitant initial s’assure 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 des articles 28 du RGPD et 96 de la loi « Informatique et Libertés » le cas échéant.

À la demande du responsable de 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 du secret des 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.

Le sous-traitant demeure pleinement responsable, à l’égard du responsable de traitement, de l’exécution des obligations du sous-traitant ultérieur, prévues par le contrat qu’il a conclu avec ce dernier. Le sous-traitant informe le responsable de traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

1. **Information et exercice des droits des personnes**

**1.** Il appartient au responsable de traitement de fournir l’information aux personnes concernées par les opérations de traitement ou de les mettre à leur disposition le cas échéant.

**2.** 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 dont les personnes le saisissent, en vue d’exercer leurs droits prévus au chapitre III du RGPD et, le cas échéant, aux articles 104 à 111 de la loi « Informatique et Libertés ».

Dans ce cadre, s'il est directement destinataire de l'une de ces demandes, le sous-traitant l'adresse, par courrier électronique et dans un délai maximum de vingt-quatre heures (24 heures) à compter de la réception de cette demande, à *[A compléter par le MINJUS/MOA : mettre l’adresse de messagerie du service du MJ qui sera en charge de traiter ces demandes ou de les adresser au bon interlocuteur (point de contact effectif des droits). Se reporter à l’AIPD le cas échéant.* *NB : Le DPD du MJ ne peut être le point d’exercice des droits pour tous les traitements du MJ].*

1. **Notification au responsable de traitement des violations de données à caractère personnel**

Il est rappelé qu’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 encore l’accès non autorisé à ces données.

En cas de violation de données, le sous-traitant coopère avec le responsable de 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 RGPD et, le cas échéant, des articles 83 et 102 de la loi « Informatique et Libertés », en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

En cas de violation de données en rapport avec des données traitées par le sous-traitant pour le compte du responsable de traitement, le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de vingt-quatre (24) heures après en avoir pris connaissance et par mail à l’adresse suivante : *[A compléter par le MINJUS/MOA : Il convient ici de veiller au canal favorisant la meilleure réactivité. Il est possible d’indiquer, par exemple, soit la même adresse électronique que celle recevant les demandes d’exercice des droits, soit toute autre adresse qui permettra d’organiser au plus vite le processus interne de remontée des violations de données au BIL/DPD-B2SI-Cellule HFDS. Cela peut par exemple être le RSSI de la direction]*.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement :

a) de documenter ladite violation, conformément à l’article 33.5 du RGPD ;

b) de disposer des informations suivantes qui, conformément à l’article 33.3, du RGPD, doivent figurer dans la notification du responsable de traitement, et inclure, au   
moins :

i- 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 ;

ii- la description des conséquences probables de la violation de données ;

iii- les mesures prises ou les mesures que le sous-traitant propose de prendre pour remédier à la violation de données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

c) de satisfaire, conformément à l’article 34 du RGPD, à l’obligation de communiquer, dans les meilleurs délais, la violation de données à la personne concernée, lorsque la violation de données est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes physiques.

S’il n’est pas possible de fournir toutes ces informations en même temps, le sous-traitant peut les communiquer de manière échelonnée, sans délai injustifié. Il en informe le responsable de traitement en lui indiquant les raisons pour lesquelles la totalité des informations ne peuvent être communiquées dans les délais initiaux.

Le sous-traitant s’engage à coopérer pleinement avec le responsable de traitement afin de l’aider dans la gestion de cette situation et notamment en :

* contribuant à la conduite des investigations sur la violation de données à caractère personnel ;
* fournissant au responsable de traitement ou à la personne qu’il a désigné, un accès physique aux installations et opérations concernées ;
* organisant des entretiens entre le personnel du responsable de traitement et son propre personnel ;
* fournissant tous les registres, journaux, dossiers, communications de données et autres documents pertinents nécessaires pour se conformer à la réglementation en vigueur et, le cas échéant, aux codes de conduite auxquels il aurait adhéré.

En tout état de cause, le sous-traitant reconnaît que le responsable de traitement est seul habilité à :

* décider si cette violation de donnée à caractère personnel doit ou non être notifiée à l’autorité de contrôle, voire communiquée aux personnes concernées ;
* formaliser le contenu de ladite notification ;
* réaliser la notification proprement dite à la CNIL, et aux personnes concernées le cas échéant.

Lorsque le responsable de traitement est dans l’obligation de communiquer la violation de données à caractère personnel aux personnes concernées, le sous-traitant prend en charge les frais liés à cette communication si la violation est survenue à cause d’un manquement de sa part aux obligations prévues par les présentes dispositions, au RGPD et à la loi « Informatique et Libertés ».

En cas de manquement du sous-traitant au titre de ses obligations décrites dans le présent article, celui-ci restaure, à ses frais, les données traitées dans le cadre du présent marché en cas de perte de données.

Ces dispositions s’appliquent sans préjudice de la procédure décrite à l’article VI.7 du CCAP relatif aux règles de sécurité applicables en cas d’attaque informatique ou d’intrusion sur les réseaux du sous-traitant, afin de s’assurer que lesdits manquements ont bien été corrigés. *[MJ/MOA : cette clause est à ajuster/supprimer le cas échéant au regard du contrat de marché public qui a été conclu. NB : Pensez à vérifier que la numérotation de l’article (VI.7 CCAP) demeure]*

Tout manquement constaté à ces obligations constitue une faute du sous-traitant et/ou de ses sous-traitants ultérieurs.

1. **Autres notifications**

Le sous-traitant doit informer le ministère dans les meilleurs délais :

* de toute demande contraignante de divulgation des données à caractère personnel, sauf si cela est interdit, par exemple dans le cadre d’une interdiction à caractère pénal visant à préserver le secret d’une enquête ;
* de toutes réclamations ou plaintes reçues directement d’une personne concernée, sans y répondre.

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

Le sous-traitant assiste le responsable de traitement pour la réalisation d’analyses d’impact relatives à la protection des données et, le cas échéant, pour le respect de l’obligation de consulter l'autorité de contrôle compétente 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, en application de l’article 36 du RGPD.

Le sous-traitant assiste également le responsable de traitement en cas de plainte formulée par une personne concernée ou par un regroupement de celles-ci ou en cas de contrôle sur place ou sur pièce de la CNIL.

1. **Mesures de sécurité encadrant le traitement des données à caractère personnel**

**1**. Le sous-traitant s’engage à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques, compte tenu 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.

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral.

Ces mesures tiennent compte de l’état de l’art, de la doctrine de la CNIL et de l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) et sont conformes aux standards de sécurité en vigueur.

**2.** A ce titre, le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées en appendice 3 pour assurer la sécurité des données à caractère personnel.

Le sous-traitant doit mettre en place lesdites mesures avant de traiter les données à caractère personnel pour le compte du ministère.

**3.** Le sous-traitant peut occasionnellement modifier les mesures techniques et organisationnelles sous réserve que les mesures techniques et organisationnelles modifiées ne soient pas moins protectrices. Tout changement substantiel sera communiqué par écrit au ministère dans un délai raisonnable.

**4.** Le sous-traitant informe son personnel et sensibilise les sous-traitants ultérieurs qui pourraient intervenir pour son compte sur les mesures de sécurité techniques et organisationnelles mises à leur charge.

Le sous-traitant n’accorde, à des personnes physiques, un 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 de la présente relation de sous-traitance.

1. **Sort des données à caractère personnel à l’issue de la prestation**

*[MJ/MOA : Le choix de l’une des deux options proposées doit se faire après vérification des obligations en matière de conservation et d’archivage du ministère sur le traitement concerné. En effet, aucune destruction définitive des données ne peut intervenir sans l’autorisation des archives. Pour ce faire, la MOA peut consulter la documentation disponible sur l’intranet du département des archives de la documentation et du patrimoine (DADP) du secrétariat général du ministère ou, au besoin, se rapprocher de ce département (SG/ARCHIVES).]*

**Option 1** : Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s’engage à renvoyer toutes les données à caractère personnel au responsable de traitement, selon les modalités de mise en œuvre spécifiées par ce dernier.

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, via un procès-verbal de destruction.

**Option 2** : Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s’engage à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement, selon les modalités de mise en œuvre spécifiées par ce dernier.

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.

1. **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 (DPD),** s’il en a désigné un conformément à l’article 37 du RGPD et de la loi « Informatique et Libertés », ainsi que toute modification afférente. Celui-ci est joignable à l’adresse suivante : *[A compléter par le sous-traitant]*

A défaut de désignation d’un DPD au moment de la signature du présent contrat, le sous-traitant fera connaître le nom et les coordonnées de son DPD dans le délai d’un mois à compter de sa désignation.

Les parties veillent à ce que le DPD soit associé en temps utile, à toutes les questions relatives à la protection des données à caractère personnel que soulèverait l'exécution des prestations.

1. **Documentation et audit**

**1.** Le sous-traitant traite de manière rapide et adéquate les demandes du responsable de traitement concernant le traitement des données conformément au présent contrat.

**2.** Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d’activités de traitement effectuées au nom et pour le compte du responsable de traitement comprenanttoutes les informations détaillées à l’article 30.2 du règlement général sur la protection des données.

Le sous-traitant s'engage à mettre le registre des catégories d’activités de traitement à sa disposition afin qu'il puisse s'assurer que les traitements de données mis en œuvre dans le cadre de l'exécution du présent accord-cadre sont conformes au RGPD et à la loi « Informatique et Libertés ».

**3.** 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.

Si les éléments mis à disposition par le sous-traitant s’avéraient insuffisants pour démontrer le respect de ses obligations au titre du présent contrat, le responsable de traitement pourra procéder, ou faire procéder par un tiers désigné par lui, à un audit sur site aux frais du sous-traitant.

Cet audit sur site sera notifié par le responsable de traitement au sous-traitant par email au minimum huit (8) jours avant la date projetée de sa mise en œuvre.

Le sous-traitant s’engage à autoriser le responsable de traitement, ou les sociétés nommées par lui auxquelles est confié l’audit, à accéder aux informations nécessaires à l’accomplissement de leur mission et à accéder aux sites où sont assurés le traitement objet de la convention. En particulier, le sous-traitant coopèrera pleinement dans le cadre de cet audit en donnant accès à du personnel averti, aux locaux, aux environnements physique et technique, à la documentation, aux infrastructures, aux logiciels d’application relatifs au traitement de données et à toutes informations utiles raisonnablement nécessaires à la réalisation de l’audit.

Si le rapport d’audit ou le rapport d’audit sur site relève une violation des termes du contrat par le sous-traitant, le responsable de traitement et le sous-traitant conviennent d’un moyen de remédier aux défaillances et de mettre en place les changements recommandés par le rapport d’audit ou le rapport d’audit sur site. En tout état de cause, le sous-traitant s’engage à fournir au responsable de traitement une première réponse sur les mesures correctives mises en œuvre dans un délai d’un (1) mois à compter de la demande de remédiation du responsable de traitement, et à corriger, de manière totale et effective, les manquements constatés dans un délai de trois (3) mois à compter de ladite demande de remédiation. Le coût de toute mesure corrective identifiée et mise en œuvre par le sous-traitant reste à sa charge.

Le responsable de traitement pourra alors procéder, ou faire procéder par un tiers désigné par lui, à un second audit de contrôle sur site aux frais du sous-traitant, afin de s’assurer que lesdits manquements ont bien été corrigés.

Si les parties ne parviennent pas à convenir d’un tel moyen ou si le sous-traitant ne s’y conforme pas dans un délai raisonnable et, en tout état de cause, dans le délai de trois (3) mois susmentionné, alors la clause « non-respect des dispositions et résiliation » trouvera à s’appliquer.

**4**. 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.

**5**. Le sous-traitant tient et met à disposition du ministère de la justice un registre des incidents de sécurité qui ont impacté les données confiées et y documente, au minimum, toute information pertinente concernant les circonstances de ces incidents de sécurité, ses effets et les mesures prises à ses frais pour y remédier et éviter qu’ils ne se reproduisent.

1. **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 III 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 RGPD et la loi « Informatique et Libertés » de la part du sous-traitant.
4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.
5. **Non-respect des clauses et résiliation**

*[MJ/MOA : Vérifier avec le bureau des marchés la possibilité d’insérer une telle clause au regard des CCTP/CCAP déjà conclus, notamment au regard des éventuelles indemnités dues en cas de résiliation anticipée]*

**1.** Sans préjudice des dispositions du RGPD et 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 de 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 de traitement s’il n’est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.

**2.** 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 :

a. le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable de traitement conformément au point 1 de la présente clause et le respect des présentes clauses n’est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai de trois (3) mois à compter de la suspension ;

b. le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du RGPD et de loi « Informatique et Libertés » ;

c. le sous-traitant ne se conforme pas à une décision contraignante d’une juridiction compétente ou des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement général sur la protection des données et de la loi « Informatique et Libertés ».

Dans ces cas, le sous-traitant ne pourra bénéficier d’aucune indemnité en se prévalant d’un préjudice résultant de l’expiration anticipée du contrat.

Pour procéder à la résiliation du contrat, le responsable de traitement procédera aux modalités décrites à l’article III.3 du CCAP.

Signature du représentant du responsable de traitement Signature du représentant du sous-traitant

A ………………, le …………………..

A ………………, le …………………..

**APPENDICE 1**

**Description du traitement**

La ou les **finalité**(s) du traitement sont de : *[A compléter par la MOA et le sous-traitant : Il s’agit d’énumérer les finalités du traitement effectués par le ST pour le compte du MJ. Si une AIPD a été réalisée, s’y reporter car elles y seront décrites. En toute hypothèse, elles doivent avoir été décrites dans la fiche de registre du traitement.]*

Les **opérations de traitement** sur les données, confiées au sous-traitant sont les suivantes : *[A compléter par la MOA et le sous-traitant : Il convient ici de décrire la nature des opérations de traitement sous-traitées (ex : collecte, enregistrement, organisation, structuration, conservation, adaptation ou modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, limitation, effacement ou destruction, hébergement, maintenance, exploitation de l’application etc.)]*

Les **catégories de personnes concernées** sont : *[A compléter par la MOA et le sous-traitant : Spécifier ici les catégories de personnes dont les données à caractère personnel sont traitées dans le cadre de la présente convention. Si une AIPD a été réalisée, s’y reporter. Les mêmes termes que l’AIPD doivent être utilisés.]*

Les catégories de **données à caractère personnel** traitées dans le cadre des opérations de traitement sous-traitées sont les suivantes : *[A compléter par la MOA et le sous-traitant : Si une AIPD a été réalisée, s’y reporter pour remplir ce passage. L’AIPD exige en effet d’être exhaustif s’agissant des données, mais il est possible de se contenter ici du type de données traitées (exemple : données d’identification, données de connexion etc.)]*

La **durée de conservation** des données est : *[A compléter par la MOA et le sous-traitant : Les données personnelles ne peuvent être conservées indéfiniment : une durée de conservation doit être déterminée en fonction de l’objectif ayant conduit à la collecte de ces données. Dans certains cas, la durée de conservation est fixée par la règlementation. Toutefois, pour de nombreux traitements de données, la durée de conservation n’est pas fixée par un texte. Il appartient alors au responsable de traitement de la déterminer en fonction de la finalité du traitement (pour plus d’informations, cf* [*https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees*](https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees)*).]*

**APPENDICE 2**

**Liste des sous-traitants ultérieurs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Identité du sous-traitant ultérieur** | **Coordonnées du sous-traitant ultérieur** | **Activités de traitement sous-traitées** | **Dates du contrat liant le sous-traitant au sous-traitant ultérieur** |
| *[A compléter par le sous-traitant]* | *[A compléter par le sous-traitant]* | *[A compléter par le sous-traitant]* | *[A compléter par le sous-traitant]* |
|  |  |  |  |
|  |  |  |  |

**APPENDICE 3**

**Mesures de sécurité techniques et organisationnelles mises en œuvre par le sous-traitant**

*Les mesures techniques et organisationnelles doivent faire l’objet d’une description concrète, et non pas générique.*

|  |  |  |
| --- | --- | --- |
| **Description des mesures contribuant à traiter des risques liés à la sécurité des données** | | |
| **Mesures portant spécifiquement sur les données du traitement** | **Attendus** | **Modalités de mise en œuvre ou justification sinon** |
| **Chiffrement** | *[Décrivez ici les moyens mis en œuvre pour assurer la confidentialité des données conservées (en base de données, dans des fichiers plats, les sauvegardes, etc.), ainsi que les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromission, etc.). Détaillez les moyens de chiffrement employés pour les flux de données (VPN, TLS, etc.) mis en œuvre dans le traitement.]* | A compléter par le sous-traitant |
| **Pseudonymisation** | *[Indiquez ici si des mécanismes de pseudonymisation sont mis en œuvre, lesquels et à quelle fin.]* | A compléter par le sous-traitant |
| **Anonymisation** | *[Indiquez ici si des mécanismes d’anonymisation sont mis en œuvre, lesquels et à quelle fin.]* | A compléter par le sous-traitant |
| **Cloisonnement des données (par rapport au reste du système d’information)** | *[Indiquez ici si un cloisonnement du traitement est prévu, et comment il est réalisé.]* | A compléter par le sous-traitant |
| **Contrôle des accès logiques** | *[Indiquez ici comment les profils utilisateurs sont définis et attribués. Précisez les moyens d’authentification mis en œuvre. Le cas échéant, précisez les règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).]* | A compléter par le sous-traitant |
| **Traçabilité (journalisation)** | *[Indiquez ici si des événements sont journalisés et la durée de conservation de ces traces.]* | A compléter par le sous-traitant |
| **Contrôle d’intégrité** | *[Indiquez ici si des mécanismes de contrôle d’intégrité des données stockées sont mis en œuvre, lesquels et à quelle fin. Détaillez les mécanismes de contrôle d’intégrité employés sur les flux de données.]* | A compléter par le sous-traitant |
| **Archivage** | *[Décrivez ici le processus de gestion des archives (versement, stockage, consultation, etc.) relevant de votre responsabilité. Précisez les rôles en matière d’archivage (service producteur, service versant, etc.) et la politique d’archivage. Indiquez si les données sont susceptibles de relever des archives publiques.]* | A compléter par le sous-traitant |
| **Sécurité des documents papier** | *[Si des documents papiers contenant des données sont utilisés dans le cadre du traitement, indiquez ici comment ils sont imprimés, stockés, détruits et échangés.]* | A compléter par le sous-traitant |

|  |  |  |
| --- | --- | --- |
| **Description des mesures générales de sécurité** | | |
| **Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre** | **Attendus** | **Modalités de mise en œuvre ou justification sinon** |
| **Sécurité de l’exploitation** | *[Décrivez ici comment les mises à jour des logiciels (systèmes d’exploitation, applications, etc.) et l'application des correctifs de sécurité sont réalisées.]* | A compléter par le sous-traitant |
| **Lutte contre les logiciels malveillants** | *[Précisez si un antivirus est installé et régulièrement mis à jour sur tous les postes.]* | A compléter par le sous-traitant |
| **Gestion des postes de travail** | *[Détaillez ici les mesures mises en œuvre sur les postes de travail (verrouillage automatique, pare-feu, etc.).]* | A compléter par le sous-traitant |
| **Sécurité des sites web** | *[Indiquez ici si les "recommandations pour la sécurisation des sites web" de l'ANSSI sont mises en œuvre.]* | A compléter par le sous-traitant |
| **Sauvegardes** | *[Indiquez ici comment les sauvegardes sont gérées. Précisez si elles sont stockées dans un endroit sûr.]* | A compléter par le sous-traitant |
| **Maintenance** | *[Décrivez ici comment est gérée la maintenance physique des équipements, et précisez si elle est sous-traitée. Indiquez si la maintenance à distance des applications est autorisée, et suivant quelles modalités. Précisez si les matériels défectueux sont gérés spécifiquement.]* | A compléter par le sous-traitant |
| **Sécurité des canaux informatiques (réseaux)** | *[Indiquez ici sur quel type de réseau le traitement est mis en œuvre (isolé, privé, ou Internet). Précisez quels système de pare-feu, sondes de détection d'intrusion, ou autres dispositifs actifs ou passifs sont chargés d'assurer la sécurité du réseau.]* | A compléter par le sous-traitant |
| **Surveillance** | *[Indiquez ici si une surveillance en temps réel du réseau local est mise en œuvre et avec quels moyens. Indiquez si un contrôle des configurations matérielles et logicielles est effectué et par quels moyens.]* | A compléter par le sous-traitant |
| **Contrôle d’accès physique** | *[Indiquez ici la manière dont est réalisé le contrôle d’accès physique aux locaux hébergeant le traitement (zonage, accompagnement des visiteurs, port de badge, portes verrouillées, etc.). Indiquez s’il existe des moyens d’alerte en cas d’effraction.]* | A compléter par le sous-traitant |
| **Sécurité des matériels** | *[Indiquez ici les mesures de sécurité physique des serveurs et des postes clients (stockage sécurisé, câbles de sécurité, filtres de confidentialité, effacement sécurisé avant mise au rebut, etc.).]* | A compléter par le sous-traitant |
| **Éloignement des sources de risques** | *[Indiquez ici si la zone d’implantation est sujette à des sinistres environnementaux (zone inondable, proximité d’industries chimiques, zone sismique ou volcanique, etc.) Précisez si la zone contient des produits dangereux.]* | A compléter par le sous-traitant |
| **Protection contre les sources de risques non humaines** | *[Décrivez ici les moyens de prévention, de détection et de lutte contre l’incendie. Le cas échéant, indiquez les moyens de prévention de dégâts des eaux. Précisez également les moyens de surveillance et de secours de l’alimentation électrique.]* | A compléter par le sous-traitant |

|  |  |  |
| --- | --- | --- |
| **Description des mesures organisationnelles (gouvernance)** | | |
| **Mesures organisationnelles (gouvernance)** | **Attendus** | **Modalités de mise en œuvre ou justification sinon** |
| **Organisation** | *[Indiquez si les rôles et responsabilités en matière de protection des données sont définis. Précisez si une personne est chargée de la mise en application des lois et règlements touchant à la protection de la vie privée. Précisez s’il existe un comité de suivi (ou équivalent) chargé des orientations et du suivi des actions concernant la protection de la vie privée.]* | A compléter par le sous-traitant |
| **Politique (gestion des règles)** | *[Indiquez ici s’il existe une charte informatique (ou équivalent) traitant de la protection des données et de la bonne utilisation des moyens informatiques.]* | A compléter par le sous-traitant |
| **Gestion des risques** | *[Indiquez ici si les risques que les traitements font peser sur la vie privée des personnes concernées sont étudiés pour les nouveaux traitements, si c'est systématique ou non, et le cas échéant, selon quelle méthode. Précisez s’il existe, au niveau de l’organisme, une cartographie des risques sur la vie privée.]* | A compléter par le sous-traitant |
| **Gestion des projets** | *[Indiquez ici si les tests des dispositifs sont réalisés sur des données fictives/anonymes.]* | A compléter par le sous-traitant |
| **Gestion des incidents et des violations de données** | *[Indiquez ici si les incidents font l’objet d’une gestion documentée et testée, notamment en ce qui concerne les violations de données à caractère personnel.]* | A compléter par le sous-traitant |
| **Gestion des personnels** | *[Indiquez ici les mesures de sensibilisation prises à l’arrivée d’une personne dans sa fonction. Indiquez les mesures prises au départ des personnes accédant aux données.]* | A compléter par le sous-traitant |
| **Relations avec les tiers** | *[Indiquez ici, notamment pour les sous-traitants amenés à avoir accès aux données, les modalités et les mesures de sécurité mises en œuvre pour ces accès.]* | A compléter par le sous-traitant |
| **Supervision** | *[Indiquez ici si l'effectivité et l’adéquation des mesures touchant à la vie privée sont contrôlées.]* | A compléter par le sous-traitant |