CONTRAT DE SOUS-TRAITANCE DU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Cet Accord fait partie du contrat entre **SYRADE** (ci-après le « Sous-traitant ») et le Client (ci-après le « Client ») pour la fourniture de solutions par SYRADE (ci-après le " Service "). Le Sous-traitant et le Client sont collectivement dénommés ci-après « les Parties ».

Tous les termes commençant par une majuscule qui ne sont pas définis au présent Accord ont la signification qui leur est donnée dans les Lois et Règlements sur la protection des données.

Dans le cadre de la fourniture du Service au Client conformément au contrat, SYRADE peut traiter des Données à caractère personnel pour le compte du Client en qualité de Sous-traitant, et les parties conviennent de se conformer aux dispositions suivantes en ce qui concerne toutes les Données à caractère personnel.

Le responsable du traitement porte une attention particulière à la protection de la vie privée de ses utilisateurs et s'engage par conséquent à prendre les précautions raisonnables requises pour protéger les données à caractère personnel récoltées contre la perte, le vol, la divulgation ou l'utilisation non autorisée.

Afin d'offrir des garanties suffisantes en matière de protection des données à caractère personnel, et plus globalement le droit à la vie privée, le responsable du traitement souhaite régler les modalités d'exécution et d'organisation du traitement de ces données.

Le responsable du traitement et le sous-traitant agissent en toute transparence, dans le respect de La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après dénommé la « loi sur la protection de la vie privée ») modifiée et 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 (ci-après dénommé le « Règlement général sur la protection des données » ou « RGPD »).

En signant la présente convention, le sous-traitant s'engage à disposer 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 de la loi sur la protection de la vie privée et du Règlement général sur la protection des données, et garantit la protection des droits de la personne concernée.

IL A ENSUITE ÉTÉ CONVENU DE CE QUI SUIT :

Définitions

Aux sens des clauses du présent contrat, on entend par :

(a) «*responsable du traitement*», 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 ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ;

(b) «*sous-traitant*», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

(c) « *données à caractère personnel* », « *catégories particulières de données* », « *traiter/traitement* », « *personne concernée* » et « *autorité de contrôle* » ont la même signification que dans le 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 (ci-après dénommé le « Règlement général sur la protection des données »).

Objet du contrat

Le responsable du traitement collecte des données à caractère personnel et souhaite confier certains aspects du traitement au sous-traitant. Dans ce contexte, le présent contrat a pour objet de régler les modalités d'exécution et d'organisation du traitement de ces données par le sous- traitant.

Il est entendu entre les parties que le sous-traitant agit exclusivement pour le compte et conformément aux instructions du responsable du traitement, et ce pendant toute la durée du présent contrat. Le responsable de traitement donne instruction au sous-traitant de procéder en son nom et pour son compte au(x) traitement(s) des données à caractère personnel décrit(s) en Annexe A – Description du traitement.

Catégorie de données traitées par le sous-traitant

L'Annexe A décrit les instructions du responsable de traitement que le sous-traitant s'engage à respecter et notamment la finalité, la durée du traitement ainsi que les catégories d'activités de traitement, les types de données à caractère personnel et des catégories de personnes concernées.

Dans l'hypothèse où des données à caractère non personnel seraient combinées à des données à caractère personnel, de sorte qu'une identification des personnes concernées serait possible, ces données seront traitées comme des données à caractère personnel jusqu'à ce que leur rapprochement avec une personne particulière soit rendu impossible.

Missions du sous-traitant

Le sous-traitant ne peut traiter les données qu'aux fins définies dans le présent contrat et

conformément aux instructions du responsable du traitement.

Dans l'éventualité où le sous-traitant serait légalement tenu d'effectuer un traitement de données en dehors des missions convenues par le présent contrat, il en informera le responsable du traitement dans les plus brefs délais.

A toutes fins utiles, il est rappelé que le responsable de traitement est le seul responsable (i) pour déterminer les finalités et les moyens du traitement des données à caractère personnel effectué par le sous-traitant ; (ii) de l'exactitude, l'adéquation et de la complétude des instructions susmentionnées. De manière expresse et générale, le sous-traitant ne détermine jamais les finalités et les moyens des traitements qui lui sont confiés par le Responsable de traitement.

Tout changement des instructions données par le responsable de traitement, notamment aux fins de mise en conformité avec les lois applicables en matière de données à caractère personnel, qui entraînerait une modification des prestations sera matérialisé par écrit et fera l'objet d'un avenant au présent contrat.

Obligations du sous-traitant

Dans le cadre de l'exécution du présent contrat, le sous-traitant s'engage à :

- garantir la confidentialité des données à caractère personnel qu'il reçoit du responsable du traitement ;
- ne peut faire une copie des données mises à sa disposition par le responsable du traitement, sauf si une copie est nécessaire pour mener pour bien sa mission conformément au présent contrat. Le sous-traitant s'engage toutefois à supprimer cette copie de manière appropriée et définitive s'il n'en a plus besoin pour l'exercice de cette mission ;
- tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant notamment : ses données d'identification, le nom et les coordonnées du responsable du traitement (et le cas échéant ceux du représentant ou de son déléguée à la protection des données) ; les catégories de traitements effectués pour le compte du responsable du traitement ; les éventuels transferts de données vers un pays tiers ou une organisation internationale ; ainsi que, dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre pour garantir la sécurité des données à caractère personnel ainsi que leur traitement ;
- mettre, le cas échéant, à la disposition de l'autorité de contrôle le registre des activités de traitement relevant de sa responsabilité.
- Le sous-traitant s'engage à respecter les mesures de sécurité en vigueur chez le responsable de traitement lors de toute intervention sur les systèmes d'information, sur site ou à distance.
- Le sous-traitant s'engage à encadrer contractuellement les obligations de ses propres sous-traitants ou intervenants tiers en matière de confidentialité et de sécurité ;
- En cas de télémaintenance permettant l'accès à distance aux fichiers du responsable de traitement, le sous-traitant ne pourra intervenir qu'après autorisation d'accès délivrée par le responsable de traitement.

Obligations du Responsable de traitement

Dans le cadre de l'exécution du présent contrat et conformément aux dispositions du RGPD, notamment ses articles 32 et 28, le Responsable de traitement s'engage à mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque lors des opérations de maintenance.

À ce titre :

- Les interventions de maintenance doivent être enregistrées dans une main courante précisant la date, la durée, la nature de l'opération et l'identité de l'intervenant ;
- Les accès à distance en télémaintenance doivent être ouverts uniquement pour une durée définie à l'avance, et immédiatement refermés à l'issue de l'intervention ;
- Toute intervention sur site doit être encadrée par un représentant du responsable de traitement. Aucun intervenant extérieur ne pourra être laissé seul dans des zones sensibles ;
- Des registres seront établis sous les responsabilités respectives du sous-traitant et du responsable de traitement, mentionnant les date et nature détaillée des interventions de télémaintenance ainsi que les noms de leurs auteurs ;
- Les données personnelles présentes sur les équipements doivent être supprimées de manière sécurisée avant tout envoi en réparation, mise au rebut ou fin de contrat de location.
- Les applications de télémaintenance doivent être choisies par le responsable de traitement avec précaution et ne doivent pas comporter de vulnérabilités connues (ex : applications qui ne chiffrent pas les communications).
- Le responsable de traitement définit et met en œuvre la politique de mots de passe déployée au sein des applications de télémaintenance. Conformément aux standards de l'ANSSI, les mots de passe doivent comporter un minimum de complexité et de robustesse et doivent respecter les recommandations suivantes :
    - Imposer une longueur minimale pour les mots de passe (moyen à fort : entre 12 et 14 caractères, fort à très fort : au moins 15)
    - Ne pas imposer de longueur maximale pour les mots de passe
    - Mettre en œuvre des règles sur la complexité des mots de passe (utilisation de majuscules, minuscules, chiffres et caractères spéciaux)
    - Choisir un mot de passe sans information personnelle ou propre à l'entreprise
    - Utiliser un mot de passe différent pour chaque service
    - Ne pas enregistrer les mots de passe en clair (au sein d'un fichier ou d'un mail par exemple)
    - Modifier les mots de passe par défaut
    - Imposer un délai d'expiration sur les mots de passe
    - Révoquer immédiatement les mots de passe en cas de compromission suspectée ou avérée
    - Mettre en place une politique de sécurité des mots de passe
    - Mettre en place un contrôle de la robustesse des mots de passe lors de leur création ou de leur renouvellement
    - Mettre à disposition un coffre-fort de mots de passe

- Le responsable de traitement s'engage à transmettre les mots de passe au sous-traitant de façon sécurisée et à ne pas transmettre ces mots de passe en clair.

Conservation des données

Le sous-traitant ne conservera pas les données plus longtemps que nécessaire pour mener à bien les missions pour lesquelles ces données sont mises à sa disposition. Lorsque la conservation n'est plus nécessaire au regard de la finalité initiale du traitement, le sous-traitant supprimera les données concernées de manière appropriée et définitive. Ceci est également valable pour les supports sur lesquels une copie des données a été conservée.

Au terme du présent contrat, le sous-traitant devra supprimer toutes les données à caractère personnel et les copies existantes, ou les renvoyer au responsable du traitement à sa demande.

Communication à des tiers

La communication à des tiers des données à caractère personnel, de quelque manière que ce soit, est interdite, sauf si ladite communication a été approuvée par le responsable du traitement.

Dans l'éventualité où le sous-traitant serait légalement tenu de communiquer les données personnelles à un tiers, il veillera à en avertir au préalable le responsable du traitement.

Sécurité des données

En application de l'article 32 du RGPD, les parties s'engagent à mettre en œuvre des mesures organisationnelles et techniques appropriées afin de garantir un niveau de sécurité adapté au traitement.

Le sous-traitant s'engage à prendre les mesures techniques et organisationnelles appropriées afin de sécuriser les données à caractère personnel et leur traitement. Dans ce contexte, il devra évaluer les risques liés au traitement ainsi que pour les droits et libertés de la personne concernée, et mettre en œuvre des mesures pour les atténuer.

Le sous-traitant veillera à ce que l'accès aux données à caractère personnel à traiter et déjà traitées soit limité aux membres du personnel employé par le sous-traitant qui ont besoin des données pour exécuter les tâches que le sous-traitant leur attribue en exécution du présent contrat.

Le sous-traitant s'engage à attirer l'attention des membres de son personnel qui ont accès aux données ou qui sont responsables du traitement sur l'importance du respect des dispositions de la loi sur la protection de la vie privée et du Règlement général sur la protection des données. Dans cette perspective, le sous-traitant leur fait signer une déclaration de confidentialité qui est jointe en annexe à leur contrat de travail.

Le sous-traitant transmettra au responsable du traitement, en Annexe B, une description des mesures techniques qu'il a mises en œuvre afin de protéger les données à caractère personnel contre la destruction, la perte, la falsification et la diffusion ou l'accès non autorisés.

Pendant toute la durée du présent contrat, le sous-traitant s'engage à respecter les principes énoncés dans la Charte de Sécurité et de Confidentialité présente en Annexe D, et ce, en raison de toutes les informations auxquelles il pourrait avoir accès dans le cadre des prestations fournies. L'Annexe D est accessible sur le site web du sous-traitant, en suivant le lien ci-contre : https://www.wavensys.fr/charte-securite-et-dpa/

Le sous-traitant doit notifier au responsable du traitement toute faille de sécurité et/ou violation de données au sens du Règlement général sur la protection des données dans les meilleurs délais après en avoir pris connaissance et au plus tard dans les 24 heures de sa constatation. Une faille de sécurité est une 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 transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

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 sous-traitant 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.

Lorsque qu'une violation de données a été constatée sur l'infrastructure ou dans les locaux du sous-traitant ou encore sur des applications dont il assure seul la maintenance, le sous-traitant s'engage à mettre rapidement des moyens en œuvre pour connaître son origine et à proposer un plan de minimisation au responsable de traitement.

Sous-traitant ultérieur

Le sous-traitant s'engage à ne pas recruter un autre sous-traitant, appelé *« sous-traitant ultérieur »*, sans l'autorisation générale du responsable du traitement.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le présent contrat sont imposées

au sous-traitant ultérieur par contrat écrit.

Le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants ultérieurs.

Lorsque le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant demeure pleinement responsable devant le responsable du traitement de l'exécution par le sous-traitant ultérieur de ses obligations.

La liste des sous-traitant ultérieurs au jour de la signature du présent contrat figure en Annexe C et devra être actualisée par le sous-traitant en cours d'exécution des prestations, le cas échéant.

Dans le cas où le sous-traitant souhaiterait sous-traiter les données à des sous-traitants ultérieurs situés en dehors de l'Espace Economique Européen (« l'EEE ») et dans un pays non reconnu comme « adéquat » au sens de la Commission Européenne, le sous-traitant met en place les garanties de transfert pour assurer un niveau adéquat de protection aux données transférées conformément au chapitre V du RGPD et en informe le responsable du traitement.

Contrôle par le responsable du traitement

Le sous-traitant s'engage à mettre à la disposition du responsable du Traitement, à sa demande expresse, toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent contrat par des moyens appropriés, conformément à l'organisation interne du sous-traitant.

Le responsable du traitement a le droit de contrôler le respect du présent contrat. À cet effet, il a la possibilité de se rendre dans les locaux ou les endroits où le sous-traitant procède au traitement des données.

Le sous-traitant s'engage à permettre la réalisation d'audits mandatés par l'autorité de contrôle compétente (la CNIL) ou par le responsable de Traitement - ou tout autre auditeur qu'il aura mandaté et qui ne saurait être un concurrent du sous-traitant – et à y contribuer.

Dans le cas où le sous-traitant est soumis à une enquête ou une demande d'informations par l'autorité de contrôle compétente, concernant l'un des traitements effectués par le sous-traitant pour le compte du responsable de traitement, le sous-traitant s'engage à en informer le responsable de traitement dans les meilleurs délais et satisfaire, dans la mesure de ses possibilités, à cette enquête ou demande.

Coopération avec le responsable du traitement et l'autorité de contrôle

Le sous-traitant coopère avec le responsable du traitement.

Dans ce cadre, il s'engage notamment à :

- assister le responsable de traitement dans le cadre de ses obligations prévues aux

articles 32 à 36 du Règlement général sur la protection des données en matière de (a) sécurité du traitement, (b) notification des incidents à l'autorité de contrôle et aux Personnes concernées et (c) étude d'impacts et consultation préalable de l'autorité de contrôle ;

- assister, dans la mesure du possible, le responsable du traitement, à sa demande et par des mesures techniques et opérationnelles, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus par la loi sur la protection de la vie privée et le Règlement sur la protection des données (droit d'accès aux données, droit de rectification, droit d'opposition, droit à l'effacement, etc.) ;
- coopérer avec l'autorité de contrôle, à la demande de celle-ci ou à la demande du responsable du traitement, dans l'exécution de ses missions ;
- signaler immédiatement au responsable du traitement s'il estime que l'une de ses instructions constitue une violation des dispositions nationales et européennes en vigueur relatives à la protection des données.

Dans le cas où la personne concernée adresse sa demande d'exercice des droits directement au Sous-traitant,

i) Le sous-Traitant informera la personne concernée que sa demande doit être adressée directement au responsable de traitement à l'adresse indiquée par lui, le responsable de traitement étant la seule personne habilitée à répondre à la demande.
ii) Le sous-traitant informera le responsable de traitement de la demande de la personne concernée et de son objet dans les meilleurs délais.

Dans le cas où le responsable de traitement sollicite l'assistance du sous-traitant pour faire droit aux demandes des personnes concernées, celle-ci relèvera des dispositions précédentes.

Responsabilités

Toute personne ayant subi un dommage matériel ou moral du fait de la violation de la loi sur la protection de la vie privée et du Règlement général sur la protection des données a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi dans sa totalité.

Lorsque le responsable du traitement et le sous-traitant participent au même traitement et qu'ils sont responsables d'un dommage causé par le traitement, le responsable du traitement ou le sous-traitant est tenu responsable du dommage dans sa totalité. Dans ce cas, celui qui a réparé totalement le dommage subi est en droit de réclamer auprès de l'autre la part de la réparation correspondant à sa part de responsabilité dans le dommage.

Le sous-traitant ne sera tenu responsable du dommage causé par le traitement que s'il n'a pas respecté le présent contrat, notamment lorsqu'il a agi en dehors des instructions licites du responsable du traitement ou contraire à celles-ci, et/ou s'il n'a pas respecté les obligations fixées par ou en vertu de la règlementation applicable sur la protection des données, sans

préjudice de sa responsabilité en vertu d'autres règles.

Le sous-traitant sera exonéré ou pourra limiter sa responsabilité, s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable. Toutefois, le sous-traitant ne peut invoquer un manquement par un sous-traitant ultérieur à ses obligations découlant du présent contrat pour échapper à ses propres responsabilités. En d'autres termes, le sous-traitant est responsable devant le responsable du traitement de la mauvaise exécution des obligations contractuelles de ses propres sous-traitants ultérieurs.

Durée et résiliation

Le présent contrat est conclu pour une durée indéterminée.

Il entre en vigueur à sa date de signature. Chaque partie pourra en outre mettre fin au contrat en notifiant cette décision par lettre recommandée et moyennant le respect d'un délai de préavis de 1 mois.

Si, pour quelque raison que ce soit, le sous-traitant n'est pas capable de respecter ses obligations en vertu du présent contrat, il s'engage à en informer immédiatement le responsable du traitement, auquel cas ce dernier aura le droit de demander au sous-traitant de suspendre les traitements de données réalisés pour son compte et/ou de résilier le contrat.

Le présent contrat est conclu en considération de la personne du sous-traitant. De ce fait, celui-ci n'a pas le droit de céder et/ou de transférer le présent contrat et/ou le droits et obligations qui en découlent à un ou des tiers, sans l'accord écrit et préalable du responsable du traitement.

Nullité d'une disposition

L'éventuelle nullité d'une disposition du présent contrat n'affecte pas la validité des autres dispositions du contrat. Les parties mettront tout en œuvre pour remplacer la disposition invalide par une disposition valide.

Loi applicable et juridiction compétente

Le présent contrat est régit par le droit national du lieu d'établissement principal du responsable du traitement.

Tout litige relatif à l'interprétation ou l'exécution de la présente Charte sera soumis aux juridictions de ce droit national.

Annexe A – Description des activités de traitement confiées au sous-traitant

Finalité du traitement :

☒ Nécessaire à la réalisation des Prestations

☐ Autre : ……..

Durée du traitement :

☒ La durée du traitement correspond à la durée du Contrat,

☐ Autre : ……

Solutions concernées :

Solution	Type d'hébergement possible (en fonction de l'offre souscrite)
Radio de télécommunication et matériels	On Premise
Radio 4G et 5G (Radio lte/4g/poc/Pttoc)	SaaS (OVH France)
Caméra piéton (body camera)	On Premise

Actions effectuées par le Sous-traitant

Activités de traitement	SaaS	On Premise
Collecte de données personnelles	☒Oui ☐Non	☐Oui ☒Non
Consultation ou lecture de données personnelles	☒Oui ☐Non	☒Oui (Support et maintenance) ☐Non
Enregistrement de fichiers de données personnelles	☒Oui ☐Non	☐Oui ☒Non
Communication de données personnelles (par transmission ou diffusion ou toute autre forme de mise à disposition)	☒Oui ☐Non	☐Oui ☒Non
Analyse de données personnelles (ex : création de statistiques)	☒Oui ☐Non	☐Oui ☒Non

Organisation ou structuration de données personnelles	☒Oui ☐Non	☐Oui ☒Non
Adaptation ou modification de données personnelles	☒Oui ☐Non	☐Oui ☒Non
Anonymisation, effacement ou destruction de données personnelles	☒Oui ☐Non	☐Oui ☒Non
Rapprochement de données personnelles (ex : croisement de données, interconnexion de données, etc.)	☒Oui ☐Non	☐Oui ☒Non
Tests impliquant des données personnelles	☐Oui ☒Non	☐Oui ☒Non
Hébergement, conservation et/ou archivage des données personnelles	☒Oui ☐Non	☐Oui ☒Non
Extraction / récupération de données personnelles	☒Oui ☐Non	☒Oui (Fin de contrat/SAV) ☐Non

Données personnelles traitées par solution

Solution concernée	Catégories de Personnes Concernées par le traitement	Catégories de Données à caractère personnel traitées	Catégories particulières de données
Radio de télécommunication et matériels	- Agents du Responsable de traitement	Nom, prénom, fonction, matricule, nom du poste de l'agent, géolocalisation	Non
Radio 4G et 5G (Radio lte/4g/poc/Pttoc)	- Agents du Responsable de traitement	Nom, prénom, fonction, matricule, nom du poste de l'agent, géolocalisation, contenu des échanges des communications	Potentiellement
Caméra piéton (body camera)	- Toute personne apparaissant sur les enregistrements vidéo	Image enregistrée et son	Potentiellement

Annexe B - Description générale des mesures de sécurité techniques et organisationnelles

Sécurité

Chiffrement :

☐ Procédure de gestion des clés et certificats

☐ Chiffrement des données

☐ Chiffrement des transmissions de données

☐ Fonction de hachage : SHA-256, SHA-512 ou SHA-3

☐ Stockage des mots de passe : HMAC utilisation SHA-256, bcrypt, scrypt ou PBKDF2

☐ Traitement de données personnelles par un sous-traitant – clause RGPD

☐ Chiffrement symétrique : AES ou AES-CBC avec clés de 128 bits

☐ Signatures : RSA-SSA-PSS comme spécifié dans PKCS#1 v2.1 avec modules et exposants secrets d'au moins 2048 bits ou 3072 bits avec des exposants publics, pour le chiffrement, supérieurs à 65536

☐ Autre : .....

Protection du réseau informatique du Sous-traitant :

☐ Limitation des accès Internet

☐ Gestion des réseaux Wi-Fi

☐ Imposition d'un VPN pour l'accès à distance

☐ Les interfaces d'administration ne sont pas accessible directement depuis Internet.

☐ Limitation des flux réseau

☐ Application des recommandations de l'ANSSI en matière de sécurisation des sites web, TLS et le Wi-Fi

☐ Identification automatique de matériels

☐ Mise en place de systèmes de détection d'intrusion

☐ Cloisonnement réseau

☐ Autre : .....

Traçabilité :

☐ Mise en place d'un système de journalisation

☐ Mise en place de protection spécifique des équipements de journalisation et des informations journalisées

☐ Mise en place d'une procédure de surveillance de l'utilisation du Traitement

☐ Examen périodique des journaux d'événement

☐ Mise en place d'une procédure de notification des anomalies ou de tout incident de sécurité

☐ Autre : .....

Gestion des habilitations :

☐ Définition de profils d'habilitation

☐ Suppression des permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique, ainsi qu'à la fin de leur contrat

☐ Réalisation d'une revue annuelle des habilitations

☐ Mise en place d'une politique de contrôle d'accès

☐ Autre : .....

Gestion des authentifications :

☐ Mise en place d'identifiant unique par utilisateur

☐ Interdiction des comptes partagés

☐ Respect de la recommandation de la CNIL du 4 septembre 2017 « Authentification par mot de passe : Les mesures de sécurité élémentaires »

☐ Authentification forte

☐ Limitation du nombre de tentatives d'accès

☐ Imposition d'un renouvellement du mot de passe

☐ Blocage du compte en cas de non renouvellement du mot de passe

☐ Utilisation des gestionnaires de mots de passe pour avoir des mots de passe différents pour chaque service ;

☐ Stockage les mots de passe de façon sécurisée

☐ Se référer aux règles et recommandations concernant les mécanismes d'authentification publiées par l'ANSSI dès lors que des mécanismes d'authentification forte sont mis en œuvre, notamment ses annexes B36 et B17 s'agissant respectivement des mécanismes d'authentification et des mécanismes cryptographiques

☐ Autre : .....

Mesures de sécurité :

☐ Utilisation d'anti-virus régulièrement mis-à-jour

☐ Mise-à-jour automatique de sécurité

☐ Rechercher la source et les traces d'intrusion en cas de compromission d'un poste

☐ Veille de sécurité

☐ Chiffrement des postes nomades et supports de stockage mobiles

☐ Mise en place de mécanismes de protection contre le vol et de limitation de ses impacts

☐ Imposition d'un VPN pour l'accès à distance

☐ Application des recommandations de l'ANSSI en matière de sécurisation des sites web, TLS et le Wi-Fi

☐ Mise en place de systèmes de détection d'intrusion

☐ Application des recommandations de l'ANSSI relatives à la sécurisation de l'administration des systèmes d'information et aux bonnes pratiques en matière de sécurisation de l'annuaire central Active Directory

☐ Mise en place d'un plan de reprise et de continuité d'activité informatique

☐ Test de la restauration des sauvegardes et de l'application du plan de continuité ou de reprise de l'activité

☐ Mise en œuvre d'une procédure de suppression sécurisée des données

☐ Utilisation de logiciels dédiés à la suppression de données certifiés par l'ANSSI

☐ Autre: .....

<u>Privacy by design/Privacy by default</u>

☐ Paramétrage par défaut et a minima par les utilisateurs de la collecte des données

☐ Non obligation de renseignement d'un champ facultatif

☐ Seules les données nécessaires à la finalité du Traitement sont collectées

☐ Purge automatique et sélective des données à la fin du Traitement

☐ Gestion des habilitations et droits d'accès informatiques « donnée par donnée » ou sur demande

☐ Autre : .....

Gouvernance des données

☐ Application des 25 référentiels de la Délibération n°2017-219 du 13 juillet 2017 de la CNIL

☐ Désignation d'un délégué à la protection des données

☐ Mise en place d'une politique appropriée en matière de protection de données

☐ Autre : .....

Formation

☐ Formation régulière aux principes de la RGPD des personnes participantes au Traitement

☐ Autre : .....

Annexe C – Liste des Sous-traitant ultérieurs

Dénomination sociale	**Activité de traitement**	**Situation géographique (Pays)**	**Moyens de transfert (pour les Sous-traitants ultérieurs hors UE)**
DESMAREZ	Mise à disposition solution (Rang 2)	France	N/A
OVH	Hébergement (Rang 3)	France	N/A
Motorola	Hébergement (POC (Rang 3)	Allemagne	N/A