|  |
| --- |
| **Contrat relatif aux données personnelles****Engagement de conformité sur le Règlement Général sur la Protection des Données 2016/679 du 27 avril 2016 (« RGPD »)** |

**ENTRE LES SOUSSIGNEES**

**Nom collectivité,** dont le siège est situé Adresse collectivité, représentée par Nom représentant, en sa qualité de Fonction du représentant

Ci-après dénommée indifféremment **le « Responsable de Traitement** »

**D'une part,**

**ET**

**Nom prestataire**, dont le siège est situé Adresse prestataire, représentée par Nom représentant, en sa qualité de Fonction du représentant ;

Ci-après dénommée indifféremment **le « Sous-Traitant »** ou « Nom prestataire »

**D'autre part,**

Le Responsable de Traitement et le Sous-Traitant/Nom prestataire sont ci-après dénommés ensemble ou séparément la ou les « Partie(s) ».

Préambule

**LE PROGRAMME SLIME**

Le CLER - Réseau pour la transition énergétique coordonne le programme SLIME - Service local d’intervention pour la maîtrise de l’énergie. Ce dispositif vise à organiser les actions de lutte contre la précarité énergétique et à massifier le repérage des ménages pour leur apporter des solutions adaptées. Créé en 2013, le programme SLIME est mis en œuvre localement par des collectivités territoriales, qui peuvent s’appuyer sur des partenaires opérationnels. La méthodologie qu’il propose s’organise en trois étapes :

1. Repérage : organisation d’une chaîne de détection des ménages en situation de précarité énergétique (ci-après les « **Bénéficiaires du SLIME** ») grâce à la mobilisation de donneurs d’alerte (travailleurs sociaux, associations, etc.)

2. Diagnostic : réalisation d’un diagnostic socio-technique lors d’une visite à domicile des ménages repérés. Ces visites permettent de conseiller les ménages sur les usages et les comportements, de fournir de petits équipements pour améliorer leur confort et favoriser les économies.

3. Orientation : accompagnement des ménages vers des solutions durables et adaptées à leur situation.

Cette méthodologie permet de centraliser les signalements de ménages et d’encourager tous les acteurs du territoire à se mobiliser et à s’organiser pour proposer des solutions variées et adaptées à chaque situation.

En 2020, une quarantaine de collectivités pilotent un SLIME, accompagnant chaque année près de 15 000 ménages.

**LE PROJET D’ETUDE D’IMPACT**

**Nom collectivité** lance un projet visant à mesurer concrètement l’impact du dispositif SLIME sur ses bénéficiaires (ci-après l’« **Etude d’Impact** »).

**Nom collectivité** ne disposant pas des moyens nécessaires, des compétences ou du savoir-faire spécifiques pour réaliser la collecte des réponses des Bénéficiaires du SLIME par le biais d’entretiens téléphoniques, a décidé de sous-traiter cette prestation à **Nom prestataire.**

Ainsi, en complément du contrat de sous-traitance signé entre **Nom collectivité** et **Nom prestataire** pour déterminer les conditions de réalisation de la collecte des réponses des Bénéficiaires du SLIME dans le contexte de la réalisation de l’Etude d’Impact, **Nom collectivité** responsable de traitement au sens « RGPD » signe le présent engagement avec **Nom prestataire** afin d’encadrer le traitement de données personnelles réalisé dans le cadre de l’Etude d’Impact (ci-après le « **Contrat** »).

**Il A ETE CONVENU CE QUI SUIT :**

**ARTICLE 1 :** **DEFINITIONS**

Les termes et expressions identifiés par une majuscule dans le cadre du Contrat, non déjà définis dans le Préambule, auront la signification mentionnée ci-après, qu’ils soient employés au singulier ou au pluriel :

« **Données** » : désigne toutes les données du Responsable de Traitement transmises au Sous-Traitant ainsi que les Données collectées, générées, manipulées ou modifiées par le Sous-Traitant dans le cadre de l’exécution des Prestations et notamment les Données à caractère personnel ainsi que les identifiants (login et mot de passe) associés à tout utilisateur autorisé au sein du Sous-Traitant.

« **Données à caractère personnel** » : désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); 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 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.

« **État de l’art** » : ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d’information publiquement accessibles, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d’information, diffusés par des organismes de référence ou encore d’origine réglementaire.

**« Evènement de Sécurité »**occurrence identifiée de l’état de service, d’un système ou d’un réseau indiquant une faille possible dans la politique de sécurité de l’information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu’alors et pouvant se relever de la sécurité de l’information.

**« Incident de Sécurité » :** est indiqué par un ou plusieurs évènement(s) de sécurité de l’information, indésirable(s) ou inattendu(s) présentant une probabilité de compromettre les opérations liées à l’activité de l’organisme et/ou de menacer la sécurité de l’information.

« **Interface d’administration** » : désigne l’interface logicielle permettant à une entité disposant des privilèges requis (un administrateur, un compte de service, etc.) de réaliser des actions d’administration et de configuration d’un système d’information.

« **Prestations** » : désigne l’ensemble des actions menées par Nom prestataire en vue de la réalisation d’une enquête de satisfaction par téléphone auprès des Bénéficiaires du SLIME.

 « **Violation de données à caractère personnel** » : [définition 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]: désigne 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.

 « **Vulnérabilité** » : désigne une faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Remarque : Une vulnérabilité peut être utilisée par un code d’exploitation et conduire à une intrusion dans le système (ANSSI).

**ARTICLE 2 : ENGAGEMENT DE CONFORMITE**

Pour les besoins du présent article, les termes suivants « données à caractère personnel », « délégué à la protection des données », « traiter/traitement », « responsable du traitement », « destinataire », « sous-traitant » et « transférer/transfert » ont la même signification que celle qui leur est donnée dans le Règlement Européen 2016/679 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 (le « **RGPD** »).

Dans le cadre de leurs relations contractuelles, les Parties s’engagent à respecter la règlementation en vigueur applicable au traitement de données à caractère personnel et en particulier le RGPD.

Au titre du Contrat, et sous réserve de dispositions contraires au titre d’un avenant ultérieur, Nom prestataire est un sous-traitant et la collectivité territoriale est responsable du traitement.

**(a) Caractéristiques du traitement**

Les caractéristiques des traitements de données à caractère personnel effectués par Nom prestataire pour le compte de la collectivité territoriale, telles que l'objet, la durée, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, sont détaillées en Annexe 1. Toute modification de l’Annexe n° 1 devra donner lieu à l’établissement d’un avenant signé par les Parties.

**(b) Obligations du Sous-Traitant**

(i) Respect des instructions du Responsable de Traitement et de la réglementation

Le Sous-Traitant s'engage à :

* traiter les données à caractère personnel collectées dans le cadre strict et nécessaire des Prestations et, d'une manière générale, à n'agir que sur la seule instruction écrite et documentée du Responsable de Traitement ;
* informer immédiatement le Responsable de Traitement si une de ses instructions constitue une violation de la réglementation applicable en matière de protection des données à caractère personnel et suspendre l’exécution de ladite instruction jusqu’à confirmation ou modification de l’instruction par le Responsable de Traitement ;
* s’assurer que les personnes autorisées à accéder aux données à caractère personnel ont connaissance des instructions du Responsable de Traitement et s’engagent à ne traiter les données à caractère personnel qui leur sont confiées que dans le strict respect de celles-ci ;
* veiller à ce que les personnes autorisées à accéder aux données à caractère personnel en vertu du Contrat reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
* désigner un délégué à la protection des données et communiquer le nom et les coordonnées de celui-ci au Responsable de Traitement ;
* ne pas concéder, louer, céder ou autrement communiquer à une autre personne, tout ou partie des données à caractère personnel, même à titre gratuit, ainsi que ne pas utiliser les données à caractère personnel à d'autres fins que celles prévues au Contrat, notamment, pour tout usage de prospection commerciale, marketing et/ou autre.
* s’agissant de ses outils, produits, applications ou services, prendre en compte les principes de protection des données dès la conception (privacy by design) et de protection des données par défaut (privacy by default) ;
* tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte du Responsable de Traitement comprenant l’ensemble des informations listées à l’article 30.2 du RGPD.

(ii) Sécurité, confidentialité, violation et destruction des données

Le Sous-Traitant s'engage à :

* prendre toutes précautions utiles afin de préserver la confidentialité et la sécurité des données à caractère personnel, et notamment, empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés, et plus généralement, à mettre en œuvre les mesures techniques et d'organisation appropriées telles que détaillées en Annexe 2 pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment, lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que, contre toute forme de traitement illicite, étant précisé que ces mesures doivent assurer, compte tenu de l'état de l'art, un niveau de sécurité approprié au regard des risques présentés par les traitements et la nature des données à protéger;
* mettre en place des habilitations pour restreindre l'accès des personnes aux données à caractère personnel et ne communiquer les données à caractère personnel qu’aux personnes ayant besoin d’en connaître, en veillant à ce que ces personnes soient soumises à une obligation contractuelle ou légale de confidentialité et de sécurité appropriée (par écrit et individuellement);
* mettre à jour les mesures de sécurité compte tenu de l’évolution de la technique, sans qu’il ne puisse résulter une diminution du niveau de sécurité et/ou un impact négatif sur la fourniture des Prestations et informer le Responsable de Traitement de toute modification substantielle des mesures de sécurité;
* notifier au Responsable de Traitement toute violation de données à caractère personnel dans les 24 heures après en avoir pris connaissance, notamment afin de permettre au Responsable de Traitement de se conformer à l'obligation prévue à l'article 33 du RGPD. Cette notification doit, à tout le moins :
1. décrire la nature de la violation de données à caractère personnel ;
2. communiquer 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 ;
3. décrire 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 ;
4. décrire les conséquences probables de la violation de données à caractère personnel ;
5. décrire les mesures prises ou que le Prestataire 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.

Les informations visées aux points c), d) et e) ci-dessus peuvent être communiquées de manière échelonnée, après la notification, sans retard indu, s’il n'est pas possible de fournir toutes les informations en même temps. ;

* mettre en place les mesures nécessaires à la protection des données à caractère personnel en cas de violation des données, en consultation avec le Responsable de Traitement pour limiter tout effet négatif sur les personnes affectées par la violation ;
* respecter les durées de conservation des données à caractère personnel, telles que spécifiées par le Responsable de Traitement ;
* détruire toutes les données à caractère personnel ainsi que communiquer au Responsable de Traitement la preuve de ces destructions.

(iii) Assistance et audit

Le Sous-Traitant s'engage, sans coût additionnel, à :

* aider et collaborer avec le Responsable de Traitement afin de garantir le respect des obligations incombant à ce dernier, conformément à la réglementation applicable en matière de protection des données à caractère personnel. Notamment, le Sous-Traitant, au titre de son devoir de conseil et au terme d’une démarche proactive, apporte toute assistance au Responsable de Traitement pour la réalisation des analyses d’impact relatives à la protection des données et pour la réalisation de la consultation préalable de l’autorité de contrôle, par exemple en lui fournissant à première demande toutes informations utiles ;
* répondre dans les 5 jours ouvrés à toute demande du Responsable de Traitement portant sur les données à caractère personnel traitées, afin de permettre au Responsable de Traitement de prendre en compte, dans les délais impartis, les éventuelles requêtes des intéressés (droit d'accès, droit de rectification, droit à l’effacement, etc.), et de manière plus générale tenir compte de la nature du traitement et aider le Responsable de Traitement par des mesures techniques et organisationnelles appropriées à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits;
* lorsque les personnes concernées exercent auprès du Sous-Traitant des demandes d’exercice de leurs droits, adresser ces demandes dès réception par courrier au contact identifié au sein du Responsable de Traitement à l’Annexe 1 décrivant les traitements. Le Responsable de Traitement assurera, à défaut d’instruction écrite contraire de sa part, le traitement de ces demandes ;
* mettre à disposition du Responsable de Traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans ce Contrat et lui incombant en tant que sous-traitant et permettre la réalisation d'audit, y compris des inspections par le Responsable de Traitement ou un autre auditeur que le Responsable de Traitement aura mandaté et contribuer à ces audits. Les audits réalisés au titre de cet article sont effectués selon les modalités prévues à l'article « Audit » du Contrat.

 **(c) Sous-traitance ultérieure**

Le Sous-Traitant s’engage à ne pas sous-traiter l'exécution des Prestations sans l'accord préalable, écrit et spécifique du Responsable de Traitement.

Le Sous-Traitant demeure en tout état de cause pleinement responsable de l'exécution, par ce sous-traitant de second rang, des obligations lui incombant et s'engage :

* à répercuter auprès de ses sous-traitants les engagements et obligations auxquels il est tenu au titre du Contrat ;
* à communiquer au Responsable de Traitement, sur demande de celui-ci, l’extrait des stipulations des contrats conclus avec ses sous-traitants de second rang portant sur la mise en œuvre de traitements de données à caractère personnel ;
* à prévoir contractuellement la possibilité pour le Responsable de Traitement d’auditer ou de faire auditer les sous-traitants de second rang dans les mêmes conditions que celles prévues à l’article Audit du Contrat.

**(d) Transferts de données à caractère personnel hors-UE**

Le Sous-Traitant s'engage que ce soit à raison des Prestations qu'il réalise ou à raison des Prestations réalisées dans le cadre d'un recours à la sous-traitance autorisée selon les conditions du Contrat, à ne pas transférer les données à caractère personnel traitées dans le cadre du Contrat, hors de l'Union Européenne ou des pays dits de « protection adéquate » sans l'autorisation préalable et écrite du Responsable de Traitement, ce dernier devant en effet pouvoir procéder, préalablement au transfert :

* + à la mise en place de garanties appropriées telles que prévues par la réglementation applicable en matière de protection des données à caractère personnel (BCR sous-traitants, clauses types de protection des données adoptées par la Commission responsable du traitement/sous-traitant, code de conduite ou mécanisme de certification approuvés),
	+ à l’inscription dans le registre des traitements et à l’obtention le cas échéant de l'autorisation préalable de transférer les données personnelles sur la base d'un engagement de l'importateur des données personnelles recueilli dans le cadre d'un mécanisme alternatif de protection des données à caractère personnel accepté par la CNIL et,
	+ à l’information des personnes concernées

Néanmoins, si le Fournisseur est tenu de procéder à de tels transferts en vertu du droit applicable, celui-ci s'engage à informer immédiatement le Client, sauf impossibilité légale.

Enfin, le sous-traitant s’engage à ne transférer aucune donnée personnelle sans un accord écrit préalable du sous-traitant quelle que soit la localisation géographique du destinataire.

Les engagements souscrits par le Sous-Traitant au titre du présent article, ne peuvent être soumis à aucune limitation de responsabilité du Sous-Traitant.

Il n’est pas autrement dérogé aux clauses et conditions du Contrat, le présent Avenant n’entraînant pas novation.

Toutes autres stipulations du Contrat, et des avenants précédents le cas échéant, qui ne seraient pas modifiées par le présent Avenant, demeurent inchangées et restent applicables. Le Contrat, les précédents avenants le cas échéant, et le présent Avenant formant un tout indissociable.

|  |  |  |
| --- | --- | --- |
| **Pour le Responsable de Traitement** |  | **Pour le Sous-Traitant** |
| Date :Nom : Qualité : Signature / cachet : |  | Date : Nom : Qualité : Signature/ cachet : |

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

* 1. Nom et coordonnées du Délégué à la Protection des Données (DPO) :

|  |  |
| --- | --- |
| **Responsable de Traitement** | **Sous-traitant(s)** |
| Nom collectivitéCoordonnées du responsable RGPD | Nom prestataireCoordonnées du responsable RGPD |

Le Sous-Traitant est autorisé à traiter, pour le compte du Responsable de Traitement, les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :

*Réalisation d’une enquête de satisfaction et d’impact par téléphone auprès des Bénéficiaires du SLIME, étant convenu que :*

* *La liste des Bénéficiaires du SLIME à contacter est communiquée par le Responsable de Traitement.*
* *Les réponses collectées par téléphone sont restituées de manière pseudonymisée à KIMSO et au Responsable de Traitement.*

La nature des opérations réalisées sur les données consiste à pouvoir identifier la personne lors du contact téléphonique et confirmer que la personne est d’accord pour répondre à l’enquête, ses réponses étant collectées de manière pseudonymisées.

La finalité du traitement est la réalisation d’une enquête de satisfaction et d’impact (désignée dans le Contrat l’« **Etude d’Impact** ») sur l’accompagnement apporté par le SLIME aux Bénéficiaires SLIME.

Le sous-traitant s’engage à préciser aux ménages contactés le contexte de l’enquête, les finalités du traitement et leurs droits concernant les données : « droit d’accès, de rectification, et d’effacement des données les concernant, de définir des directives relatives au sort de celles-ci après leur décès et de limitation du traitement et au retrait de leur consentement en s’adressant à Coordonnées du responsable RGPD de la collectivité. »

Les données à caractère personnel traitées sont :

|  |  |
| --- | --- |
| **Catégorie de données**  |  |
| **Etat civil, identification, données d’identification, image :*** Nom
* Prénom
* Numéro de téléphone
 | Oui |
| **Vie personnelle :*** Composition du ménage
* Changement dans la situation d’emploi
* Habitudes de consommation d’énergie, montant des factures et mise en place d’écogestes
* Remplacement d’équipements électro ménagers
* Conduite de travaux
* Situation dans le logement
 | Oui |
| **Vie professionnelle** (cv, scolarité, formation professionnelle, distinctions…) | Non |
| **Informations d’ordre économique et financier :*** Revenu fiscal de référence
* Allocations et montant
* Difficulté à payer des factures / situation d’impayé
 | Oui |
| **Données de connexion** (adresse IP, logs…) | Non  |
| **Données de localisation** (déplacements, données GPS, GSM…) | Non  |
| **Données sensibles** (données de santé ; numéro de sécurité sociale ; données relatives aux infractions, condamnations et mesures de sécurité ; opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, origines raciales ou ethniques)  | Non |

Les catégories de personnes concernées sont des bénéficiaires du dispositif SLIME, personnes physiques.

Pour l’exécution de la prestation objet du Contrat, le Responsable de Traitement met à la disposition du Sous-Traitant les instructions nécessaires suivantes :

* Durée du traitement : le temps de la réalisation de l’Etude d’Impact. Le Comité de Pilotage se réunira à la fin de l’étude pour clore cette étude.
* Durée de conservation des données : le temps de la réalisation de l’Etude d’Impact, au plus tard jusqu’au **Date de fin de l’Etude d’impact.**
* Sort des données au terme de la Prestation : suppression de toutes les données communiquées par le Responsable de Traitement et puis collectées (de manière pseudonymisée) auprès des personnes interrogées dans le cadre de l’Etude d’Impact. Un certificat de destruction des données, ainsi qu’une preuve de la destruction des données, seront à communiquer par le Sous-Traitant au Responsable de Traitement.

**ANNEXE 2 : Sécurité des données à caractère personnel**

* 1. Politique de sécurité de l’information

Le Sous-Traitant documente, met à jour régulièrement et tient à la disposition du client les documents relatifs à la sécurité de l’information, notamment :

- La stratégie de sécurité de l’information et sa déclinaison en mesures opérationnelles

- Le plan de mise en conformité au RGPD

- Les éventuelles certifications de sécurité

* 1. Organisation de la sécurité de l’information

Le Sous-Traitant met en œuvre une organisation de sécurité de l’information et alloue les ressources nécessaires à la définition des responsabilités, au cloisonnement des tâches, à la mise en œuvre des actions de sécurité physiques et logiques et rend compte au client des éventuels incidents.

Le Sous-Traitant s’engage sur les mesures nécessaires à la sécurisation des postes de travail et des équipements mobiles utilisés par ses personnels et ses sous-traitants dans l’exécution du contrat afin que ces équipements ne constituent pas un vecteur d’atteinte à la sécurité de l’information ; notamment par une limitation de l’accès aux données (chiffrement des équipements, verrouillage automatique de session notamment sur les temps de pause…).

Le Sous-Traitant s’engage à stocker les données personnelles, reçues du Responsable de Traitement, uniquement sur le logiciel de transfert et de stockage via le logiciel 7-zip.

Le Sous-Traitant s’engage à saisir de manière pseudonymisée les réponses aux questionnaires adressés par téléphone aux bénéficiaires du SLIME, et à transférer ces données pseudonymisées au cabinet KIMSO.

* 1. La sécurité des Ressources Humaines

Le Sous-Traitant veille à faire respecter les règles de sécurité et de confidentialité avant le démarrage des services, notamment au travers de clauses de confidentialité dans le contrat de travail ou la signature d’une charte de confidentialité.

Le Sous-Traitant veille à ce que les exigences en termes de sécurité et de confidentialité du système informatique (hébergeant les Données du Responsable de Traitement) et de protection des données soient diffusées auprès de chaque intervenant, sous-traitants inclus.

Le Sous-Traitant veille à ce que tout intervenant reçoive une formation, incluant les exigences RGPD ainsi que les spécificités des populations interrogées, adaptée à sa fonction opérationnelle et soit sensibilisé régulièrement à la protection des données du Responsable de Traitement.

A la fin du contrat, les intervenants doivent restituer au Sous-Traitant le matériel et les informations relatifs au Responsable de Traitement qui leur ont été remis pour le bon déroulement des Prestations ; les droits spécifiques des administrateurs systèmes et applicatifs sont révoqués.

* 1. Gestion des actifs

Le Sous-Traitant dispose et tient à jour un inventaire des supports informatiques où sont traités ou stockées les Données du Responsable de Traitement.

En cas d’échéance ou de résiliation du Contrat, le Sous-Traitant permet au Responsable de Traitement de récupérer une copie de l’intégralité des données dans un format exploitable par le Responsable de Traitement, puis dans un second temps à détruire toutes les copies des Données détenues dans ses systèmes informatiques.

Le Sous-Traitant protège la confidentialité des données sur les médias amovibles et lors des transferts à des tiers autorisés. Au terme de l’utilisation d’un matériel informatique par le Sous-Traitant (notamment en cas de mise au rebut, vente, réattribution ou recyclage) utilisé dans le cadre de la Prestation et plus particulièrement pour les matériels de stockage, aucune donnée ne doit rester sur celui-ci qui pourrait entraîner la divulgation d’informations du Responsable de Traitement.

* 1. Contrôle d’accès

Le Sous-Traitant établit une politique de contrôle d’accès sur la base des enjeux de sécurité et en définissant des profils d’habilitations.

Il met en place des procédures formelles pour contrôler les droits d’accès aux systèmes et services d’information du Sous-Traitant (hébergeant les Données du Responsable de Traitement) couvrant tout le cycle de vie de l’accès utilisateur, incluant une revue au minimum annuelle des droits et des comptes d’accès.

Le Sous-Traitant met en œuvre :

- les moyens nécessaires pour garantir l’unicité des identités des utilisateurs

- une politique de mot de passe utilisateur conforme aux recommandations de la CNIL

- une limitation du nombre de tentatives d’accès présentant un authentifiant erroné

Le Sous-Traitant met en œuvre un dispositif de séparation garantissant l’étanchéité des environnements utilisateurs et des Données dans les environnements support et sous toutes leurs formes (stockage, mémoire, transmission, ...). Le Sous-Traitant différencie l’Interface d’administration de l’interface permettant l’accès des utilisateurs finaux.

* 1. Cryptographie

Le Sous-Traitant met en œuvre des méthodes de chiffrement basés sur des standards publics éprouvés, à l’état de l’art, permettant à toute donnée client d’être notamment transmise de façon sécurisée. Les secrets et les clés cryptographiques sont conservés de manière sécurisée.

* 1. Sécurité physique et environnementale

Des périmètres de sécurité sont définis et utilisés pour protéger les zones contenant l’information sensible. Le Sous-Traitant applique des mesures de sécurité physique aux bureaux, aux salles et aux équipements, en particulier pour se protéger des désastres naturels, d’attaques malveillantes ou d’accidents.

* 1. Sécurité liée à l’exploitation

Le Sous-Traitant met en œuvre et contrôle les procédures d’exploitation, en particulier celles relatives à la mise à jour des systèmes, aux applications, aux processus d’administration, de développement et de sécurité des développements, à la séparation des environnements de test, de recette et de production.

Le Sous-Traitant met en œuvre des systèmes de détection d’intrusion pour faciliter la détection rapide, l’investigation et la résolution des incidents de sécurité ; notamment des solutions de lutte contre les codes malveillants.

Le Sous-Traitant installe les correctifs logiciels le plus tôt possible sur ses applications et ses systèmes. Une politique de sauvegarde des données est définie précisant la fréquence et durée de rétention. Les sauvegardes des données stockées sur les moyens du Sous-Traitant sont sous sa responsabilité. Le Sous-Traitant mène des tests de restauration réguliers. Les Données sauvegardées à l’extérieur sont au préalables chiffrées.

Le Sous-Traitant met en œuvre des capacités de surveillance et de détection des traitements non autorisés de l’information, notamment des violations de données ; il avertit le Responsable de Traitement dès qu’il détecte une vulnérabilité avérée. Des traces informatiques permettent de suivre les éventuels changements intervenus sur les données à caractère personnel. Le Sous-Traitant s’engage à mettre en place des mesures nécessaires à leur protection et notamment à restreindre les accès physiques et logiques, de son personnel et de ses sous-traitants au journal d’événements sécurisés aux seules personnes habilitées à cet effet.

* 1. Sécurité des communications

Le Sous-Traitant limite les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Le Sous-Traitant limite les accès Internet en bloquant les services non nécessaires.

Les réseaux Wi-Fi utilisent un chiffrement à l’état de l’art (WPA2 ou WPA2-PSK) et les réseaux ouverts aux invités sont séparés du réseau interne.

Le Sous-Traitant impose un VPN pour l’accès à distance et s’assure qu’aucune interface d’administration n’est accessible directement depuis Internet.

Le Sous-Traitant met en œuvre la version la plus récente du protocole TLS sur tous les sites web et rend son utilisation obligatoire pour toutes les pages d’authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.

Les pièces sensibles transmises via la messagerie électronique sont chiffrées et la clé de chiffrement est transmise via un canal distinct (par exemple par SMS).

* 1. Acquisition, développement et maintenance des systèmes d’information

Les exigences liées à la sécurité des systèmes d’information doivent être intégrées aux exigences des nouveaux développements et à la maintenance des systèmes existants.

Le Sous-Traitant met en place des frameworks et bonnes pratiques (par exemple, OWASP) pour le développement sécurisé d’applications internet et intranet. Le Sous-Traitant s’engage à réaliser une phase de test et de recette de sécurité couvrant les vulnérabilités majeures (OWASP, MITRE, ...).

Le Sous-Traitant met en œuvre sur les services des mécanismes de verrouillage des sessions applicatives et de déconnexion automatique.

Les données de production (notamment les données à caractère personnel) ne peuvent pas servir de données de test à moins d’avoir été anonymisées (ou pseudonymisées) auparavant.

* 1. Relations avec les Sous-Traitant

Le Sous-Traitant tient à disposition du Responsable de Traitement une cartographie exhaustive de l’ensemble de ses sous-traitants.

* 1. Gestion des incidents liés à la sécurité de l’information

Le Sous-Traitant s’impose la mise en place d’un processus de gestion des incidents incluant :

- Des procédures de signalement des évènements et incidents de sécurité auprès du Responsable de traitement

- La sensibilisation de ses intervenants à ces procédures

Le Sous-Traitant définit, met en œuvre et teste un dispositif de gestion de Violations de Données à Caractère Personnel.

Il s’engage notamment à notifier au Client toute Violation de la confidentialité des données à caractère personnel sous 24 heures dès sa détection.

Il garde un journal avec la description de l’incident et des données compromises (si connues), les coordonnées du déclarant et de la personne à qui l’incident a été communiqué, les mesures prises pour le résoudre (personnes en charge, et les données qui ont pu être récupérées), les éventuelles conséquences (pertes, divulgation, altération) qui en ont résulté.

* 1. Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité

Le Sous-Traitant dispose d’un Plan de continuité de l’activité (PCA) en qu’il maintiendra pendant toute la durée du contrat, afin de garantir la continuité des Prestations.

* 1. Conformité

Le Sous-traitant a mis en place et maintient un plan et processus de contrôle en matière de sécurité de l’information.

A la demande du Responsable de Traitement, le Sous-Traitant fournira un rapport d’évaluation (test d’intrusion, audit sécurité…) et le plan d’action associé.