ANNEXE A : CONDITIONS GÉNÉRALES EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Classification:
Document confidentiel

Version:
1.1 (13/12/2019)

1. Définitions

Les définitions de l'article 4 du RGPD sont applicables aux conditions générales.

Sans préjudice des définitions prévues dans les autres parties du contrat, les définitions ci-après commençant avec une majuscule ont les définitions ci-après :

"Contrat" fait référence au Contrat cadre de services de la plateforme mySecu ainsi qu'à ses annexes. Les définitions reprises dans le Contrat valent également pour les annexes ;

"Conditions générales" fait référence aux présentes Conditions générales en matières de protection des données à caractère personnel ;

"Destinataire" signifie la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ;

"Données Personnelles" signifie toute donnée à caractère personnel telle que définie dans les Lois Données Personnelles, qui fait l'objet ou qui est susceptible de faire l'objet d'un traitement par n'importe quelle Partie pour ou par l'intermédiaire d'une autre Partie, or par cette Partie directement. Les Données Personnelles incluent toute information se rapportant à une personne physique identifiée ou identifiable; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro 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 ;

"Instruction" signifie les instructions écrites et documentées, émanant du Responsable du traitement à destination du Sous-traitant, définissant les actions à prendre concernant les Données Personnelles. Les Instructions doivent initialement être spécifiées dans le Contrat et peuvent, le cas échéant, faire l'objet d'amendements, de modifications ou être remplacées par le Responsable du traitement dans des documents écrits séparés ;

"Incident de sécurité" signifie tout incident existant ou suspecté : (i) la perte, la destruction ou le vol de Données Personnelles volontaire ou accidentel ; (ii) l'utilisation, la divulgation, l'accès, l'acquisition, l'altération, la transmission ou l'accès non autorisé, ou tout autre traitement non autorisé de Données Personnelles qui peut raisonnablement compromettre la vie privée ou la confidentialité des Données Personnelles ; ou (iii) l'impossibilité d'accéder aux systèmes, pouvant résulter d'une infection malicieuse de ces systèmes, qui peut raisonnablement compromettre la vie privée ou la confidentialité des Données Personnelles. Un Incident de sécurité inclut, sans que la liste soit limitative, une attaque de type "ransomware", "denial-of-service" ou tout autre incident similaire dont il découle qu'une tierce partie prend le contrôle des systèmes ou empêche le Sous-traitant de fournir les services auxquels il s'est engagé dans le Contrat.

"Lois Données Personnelles" signifie le respect de la législation en vigueur en matière de protection des données à caractère personnel;

"Personne concernée" signifie la personne physique dont les Données Personnelles sont traitées ;

"Responsable du traitement" signifie 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 ;

"Sous-traitant" signifie la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel au nom et pour le compte du Responsable du traitement ;

"Tiers" signifie une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable de traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du Responsable de traitement ou du Sous-traitant, sont autorisées à traiter les données ;

"Traitement", "**Traitant**" ou "**Traité**" toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

3 Obligations du responsable de traitement

Le Responsable du traitement et le Sous-traitant sont tous les deux responsables du respect et de la conformité aux dispositions des Lois Données Personnelles pour les dispositions qui les concernent.

Le Responsable du traitement supporte la responsabilité primaire de s'assurer que le traitement est légitime.

En conséquence, le Responsable du traitement est personnellement responsable :

(i) de l'enregistrement des activités de traitement réalisées sous sa responsabilité ;
(ii) de la mise en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément aux Lois Données Personnelles. Pour ce faire, le Responsable du traitement tient compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, que présente le traitement pour les droits et libertés des personnes physiques. Ces mesures sont réexaminées et actualisées si nécessaire ;
(iii) de la suite à donner aux demandes dont les Personnes concernées le saisissent en vue d'exercer leurs droits;
(iv) coopère avec le Sous-traitant ;
(v) dénonce les violations de données aux autorités de supervision dans les délais impartis.

L'Entité cliente et les Tiers auxquels les Données Personnelles sont transmises sont à leur tour Responsable du Traitement de ces Données et sont, de ce fait, tous les deux responsables du respect et de la conformité aux dispositions des Lois Données Personnelles pour les dispositions qui les concernent.

Ils supportent la responsabilité de s'assurer que le traitement est légitime et sont personnellement responsables des mêmes obligations que celles reprises ci-dessus (i à vi).

4 Obligations du sous-traitant

Lorsqu'un traitement doit être effectué pour le compte du Responsable du traitement par un Sous-traitant, ce dernier ne traite les Données Personnelles que sur instruction documentée du Responsable du traitement et :

(i) respecte la stricte confidentialité des Données Personnelles;
(ii) veille à ce que les personnes autorisées à traiter les Données Personnelles s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;
(iii) prend toutes les mesures de sécurité requises en vertu de l'article 32 du RGPD ;
(iv) respecte toutes les règles du point 8 des conditions générales lorsqu'il recrute un autre sous-traitant ;
(v) aide le Responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les Personnes concernées le saisissent en vue d'exercer leurs droits;
(vi) selon les décisions du Responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au Responsable du traitement au terme de la prestation de services; et
(vii) met à la disposition du Responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues aux articles 32 à 36 du RGPD.

Les mesures reprises ci-avant sont détaillées aux articles suivants.

Le Sous-traitant informe immédiatement le Responsable du traitement si, selon lui, une Instruction constitue une violation des Lois Données Personnelles.

5 Confidentialité

Le Sous-traitant s'engage à traiter les Données Personnelles comme des données confidentielles.

Le Sous-traitant veille à la confidentialité des Données Personnelles conformément aux Lois Données Personnelles, y compris en ce qui concerne l'accès aux Données Personnelles par une tierce partie, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis; dans ce cas, le Sous-traitant (i) informe le Responsable du traitement de cette obligation juridique avant le traitement, et (ii) veille à limiter cette divulgation au strict nécessaire.

Le Sous-traitant veille à imposer les obligations de confidentialité à tous les membres de son personnel ainsi qu'aux Sous-traitants auxquels il a recours le cas échéant.

6 Transfert de données personnelles

Le Sous-traitant s'engage à conserver les Données Personnelles sur le territoire de l'Espace Economique Européen (EEE).

Le Sous-traitant s'engage et veille dans ce contexte en particulier à ce que :

- Le Sous-traitant et ses sous-traitants n'accèdent pas aux Données Personnelles via un accès remote à partir d'un endroit situé en dehors de l'EEE sauf Incident de sécurité grave pouvant affecter les Données Personnelles, auquel cas cet accès est strictement réservé aux seuls administrateurs autorisés dans le cadre de la gestion des incidents ;
- Le Sous-traitant ne procède au transfert de Données Personnelles en dehors de l'EEE ou d'un Etat ou à une organisation que lorsque celle-ci présente 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 des Lois Données Personnelles. Avant de procéder à un tel transfert, le Sous-traitant demande l'autorisation écrite du Responsable du traitement. Dans ce cas, le transfert autorisé en-dehors de l'EEE doit être suffisamment documenté et découler d'une obligation légale, dans le respect des Lois Données Personnelles.

Si le Sous-traitant découvre ou a de fortes raisons de croire que des Données Personnelles ont été traitées en dehors de l'EEE dans le non-respect de la présente disposition, il doit en informer rapidement le Responsable du traitement.

7 Sous-traitance en cascade

Recrutement d'un sous-traitant par le Sous-traitant.
Le Sous-traitant ne recrute pas un autre sous-traitant (« Sous-traitant ultérieur ») sans l'autorisation écrite préalable du Responsable du traitement. Dans le cas d'une autorisation écrite générale, le Sous-traitant informe le Responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au Responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements. Lorsqu'il recrute un autre sous-traitant pour mener des activités de traitement spécifiques, le Sous-traitant impose les mêmes obligations en matière de Données Personnelles que celles fixées dans le contrat ou tout autre acte juridique entre le Responsable du traitement et le Sous-traitant. Ces obligations doivent être imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique. Le sous-traitant a l'obligation de recruter un sous-traitant ultérieur qui dispose des mêmes garanties que lui.

Liste des sous-traitants du Sous-traitant.
Le Sous-traitant tient à la disposition du Responsable du traitement une liste de ses sous-traitants qu'il s'engage à lui remettre à première demande.

Responsabilité.

Lorsque le Sous-traitant ultérieur recruté par le Sous-traitant ne remplit pas ses obligations en matière de protection des Données Personnelles, le Sous-traitant initial demeure pleinement responsable vis-à-vis du Responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations.

8 Sécurité

Le Sous-traitant doit présenter des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences des Lois Données Personnelles (article 24).

Il doit également respecter les obligations découlant des articles 32 à 36 du Règlement Général sur la Protection des Données (Règlement EU 2016/679). De telles mesures doivent garantir un niveau de sécurité adapté au risqué, y compris entre autres, selon les besoins :

Programme de sécurité.
Le Sous-traitant s'engage à maintenir ou à faire en sorte qu'un programme de sécurité de l'information raisonnable tenant compte des règles de l'art soit conforme aux Lois Données Personnelles et qu'il soit conçu pour assurer de manière raisonnable la sécurité et la confidentialité de toutes les Données Personnelles.

Mesures de sécurité.
Le Sous-traitant s'engage à prendre toutes les mesures appropriées adaptées aux règles de l'art, y compris, sans s'y limiter, les garanties administratives, physiques, techniques (y compris électroniques) et procédurales. Ces garanties doivent notamment inclure le cryptage des données en transit. Pour les informations traitées sous forme électronique, le Sous-traitant convient que de telles garanties doivent inclure, notamment, des pare-feu et des mécanismes d'authentification et de gestion des accès aux Données Personnelles. Le Sous-traitant doit s'assurer que les Données Personnelles ne sont disponibles que pour le personnel du Sous-traitant qui a un besoin légitime d'y accéder, moyennant la signature de contrat de confidentialité.

Le Sous-traitant met en œuvre et maintient toutes les garanties de sécurité et de confidentialité supplémentaires, qui lui sont imposées par le Responsable du traitement, en cas de (i) changement matériel ou technologique ; (ii) Incident de sécurité ; ou (iii)la découverte d'une vulnérabilité ou d'une faiblesse importante ayant un impact sur la vie privée ou sur la sécurité.

De telles mesures peuvent inclure :

- La pseudonymisation des Données Personnelles ;
- Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- Des moyens permettant de rétablir la disponibilité des Données Personnelles et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Conflits.
En cas de conflit entre l'obligation d'employer et de maintenir un programme de sécurité de l'information, l'obligation de se conformer aux normes, aux instructions ou aux obligations liées à la vie privée ou à la sécurité contenues dans le Contrat, le Sous-traitant doit se conformer aux obligations qui assurent la plus grande protection pour les Données Personnelles.

9 Notification

En cas de violation de Données Personnelles, le Responsable du traitement doit notifier la violation en question à l'autorité de contrôle compétente, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Le Sous-traitant s'engage à aider le Responsable du traitement dans le contexte d'une telle notification de violation de données à l'autorité de contrôle compétente.

A ce titre, le Sous-traitant notifie dans les meilleurs délais et, impérativement, dans les 72 heures au Responsable du traitement, par écrit, toute violation de Données Personnelles ou tout Incident de sécurité dont il a pris connaissance.

Lors d'un Incident de sécurité, le Sous-traitant, sur instruction du Responsable du traitement, que cela soit ou non requis par les Lois Données Personnelles, informera par écrit les personnes concernées dont les données sont impactées par l'Incident de sécurité, et tiendra le Responsable du traitement quitte et indemne de tous les dommages directs et financiers découlant d'une telle information.

Aucune limitation ou exclusion dans le Contrat ne limite les droits du Responsable du traitement de réclamer des dommages-intérêts pour les pertes ou les sanctions subies par le Responsable du traitement suite au manquement par le Sous-traitant à ses obligations légales et contractuelles. En cas de procédure intentée par un procureur général de l'État ou par une autre autorité gouvernementale à l'encontre du Responsable du traitement pour un Incident de sécurité dont le Sous-traitant est responsable, ce dernier se substituera au Responsable du traitement dans le cadre du litige et assumera les frais de justice encourus par le Responsable du traitement.

Le Sous-traitant reconnaît que le Responsable du traitement conserve l'autorité exclusive et le pouvoir discrétionnaire de contacter et d'impliquer les autorités dans le cadre d'un Incident de sécurité, lorsqu'une telle décision est discrétionnaire (c'est-à-dire lorsque aucune obligation légale, statutaire ou autre n'oblige l'une des parties à contacter une autorité quelconque). Si le Responsable du traitement décide de contacter les autorités compétentes concernant un Incident de sécurité, le Sous-traitant s'engage à coopérer pleinement avec ces autorités.

10 Demande d'accès

Le Sous-traitant informe immédiatement le Responsable du traitement de toute demande d'accès aux Données Personnelles émanant d'une autorité officielle ou d'une tierce personne. Le Sous-traitant informe le Responsable du traitement de tout mandat, citation à comparaître ou toute autre demande relative aux Données Personnelles au plus tard cinq (5) jours ouvrables suivant la réception de la demande, sauf interdiction légale. Le Sous-traitant se conforme aux injonctions de préservation du Responsable du traitement et collabore avec le Responsable du traitement.

Le Sous-traitant assiste le Responsable du traitement suite aux demandes dont les autorités ou les Personnes concernées le saisissent en vue d'exercer leurs droits.

11 Rétention, retour et destruction des données personnelles

Rétention des données pendant l'activité.
mySecu offre trois différents types de durée de rétention :

- Une durée de rétention variable qui est définie lors de la création de la demande par l'Utilisateur final et qui sera appliquée automatiquement par le système mySecu.
- Une durée de rétention définie par le cycle de vie du Service.
- Une durée de rétention nulle dans la mesure où aucune donnée n'est stockée.

Retour et destruction.
Lorsque le Service est interrompu, le sous-traitant :

- Coupe l'accès aux Données Personnelles du Service,
- Retire les Données de la plateforme,
- Conserve les Données Personnelles dans un format autre que celui délivré par la plateforme, sur un back-up hors ligne disponible manuellement durant une période limitée à la période de rotation des tapes de backup. Passé ce délai, les données sont effacées.

La résiliation du Contrat n'entraîne pas nécessairement l'interruption du Service.

Backup.
Sauf dispositions contraires, le Sous-traitant met en œuvre, tous les jours, les mesures nécessaires pour sauvegarder les Données Personnelles. Les Données Personnelles sauvegardées sont stockées à deux (2) emplacements géographiques distincts ou plus. Les copies de sauvegarde sont utilisées par le Sous-traitant et ses agents uniquement à des fins de sauvegarde. Pour des raisons techniques, les backups sont susceptibles de contenir des données dont la durée de rétention a été dépassée mais l'accès à ces données est strictement restreint.

12 Audit

Le Sous-traitant s'engage à maintenir un niveau de sécurité adéquat et à tester la sécurité de la plateforme une fois par an.

Le Sous-traitant documente toutes les activités de traitement qu'il effectue pour le compte du Responsable du traitement conformément aux Lois Données Personnelles, notamment, sans que la liste ne soit limitative, la tenue d'un registre des traitements, les informations concernant les transferts de données transfrontaliers ainsi qu'une description générale des mesures de sécurité mises en œuvre à l'égard des Données Personnelles traitées. Le Sous-traitant doit fournir au Responsable du traitement toutes les informations nécessaires pour démontrer sa conformité aux Lois Données Personnelles.

13 Divers

Les présentes Conditions générales en matière de protection des données à caractère personnel remplacent toute disposition du Contrat dans la mesure où une telle disposition se rapporte à la vie privée, à la confidentialité ou à la sécurité des Données Personnelles; toutefois, en cas de conflit entre les dispositions des Conditions générales en matière de protection des Données Personnelles et les autres parties du Contrat, le Sous-traitant respectera les obligations qui offrent la plus grande protection aux Données Personnelles.

EN FOI DE QUOI la présente Annexe a été signée à Luxembourg le…….. par les représentants dûment autorisés des trois (3) Parties en trois (3) exemplaires originaux, un (1) pour chaque Partie.

Pour le Sous-traitant	Pour le Prestataire de Services	Pour l'Entité cliente
Par :	Par :	Par :
Fonction :	Fonction :	Fonction :