Annexe de traitement des données

Cette annexe de traitement des données (l'« **Annexe de Traitement des Données** ») contient les dispositions concernant la protection des données à caractère personnel applicables à la convention conclue entre la Société (le « **Sous-traitant** ») et le Client (le « **Responsable** ») (la « **Convention** ») et fait partie intégrante de la Convention. Le Responsable bénéficie du service offert par le Sous-traitant (le « **Service »**) dans le cadre la Convention).

Le Responsable et le Sous-traitant sont désignés individuellement comme « **partie** » et collectivement comme « **parties** ».

Lorsqu'il fournit le Service au Responsable en vertu de ou en lien avec la Convention, le Sous-traitant est susceptible de traiter des Données Personnelles en provenance du Responsable. Le Responsable et le Sous-traitant souhaitent fixer dans l'Annexe de Traitement des Données le cadre du traitement des Données Personnelles par le Sous-traitant en vertu de ou en lien avec la Convention.

Les parties conviennent ce qui suit :

1. Interprétation

1.1. Dans l'Annexe de Traitement des Données :

- « **Données Personnelles** » désigne les données à caractère personnel qui dans le cadre de la fourniture du Service font l'objet d'un traitement par le Sous-traitant en capacité de sous-traitant (à l'exclusion des données à caractère personnel que le Sous-traitant traiterait dans ce cadre en capacité de responsable du traitement). Une description des Données Personnelles est reprise à l'annexe 1 ;
- « **Incident de Sécurité** » désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de, ou l'accès non autorisé à, des Données Personnelles ;
- « **Législation sur la Protection des Données Applicable** » désigne tout acte législatif ou réglementaire relatif au traitement des Données Personnelles applicable au Responsable, au Sous-traitant ou au Service en ce compris la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et le Règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (Règlement Général sur la Protection des Données) (le « **RGPD** »), la Loi du 13 juin 2005 relative aux communications électroniques et tout autre instrument transposant la Directive 2002/58 du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dans chaque cas tel qu'en vigueur et applicable, et tel qu'éventuellement modifié, complété ou remplacé de temps en temps ;
- « **Pays Tiers** » désigne un pays situé en dehors de l'Espace Économique Européen ;

- « **Personne Concernée** » désigne la personne physique identifiée ou identifiable au moyen des Données Personnelles ;
- « **Représentants** » désigne les représentants, administrateurs, travailleurs, préposés, consultants du Sous-traitant et les autres personnes agissant sous son autorité ou sous son contrôle à qui la divulgation des Données Personnelles est strictement nécessaire pour la fourniture du Service ;
- « **Sous-traitants Approuvés** » désigne les sous-traitants (de second rang) qui ont été approuvés par le Responsable conformément à l'Annexe de Traitement des Données.

1.2. En cas de conflit ou d'incohérence entre une disposition de l'Annexe de Traitement des Données et une disposition dans la Convention, la disposition de l'Annexe de Traitement des Données prévaudra sur l'autre.

2. Conformité à la Législation sur la Protection des Données Applicable

2.1. Lors du traitement des Données Personnelles, chaque partie se conforme à ses obligations en vertu de la Législation sur la Protection des Données Applicable.

2.2. Le Sous-traitant traite les Données Personnelles de la manière et aux fins énoncées à l'annexe 1 et, le cas échéant, uniquement dans la mesure nécessaire pour se conformer à une obligation légale applicable au Sous-traitant.

2.3. Le Responsable donne instruction au Sous-traitant de traiter les Données Personnelles pour le compte du Responsable uniquement dans la mesure raisonnablement nécessaire à la fourniture du Service et autorise le Sous-traitant à fournir pour le compte du Responsable aux Sous-traitants Approuvés une instruction équivalente à l'instruction qu'il a reçue.

2.4. Si, de l'opinion raisonnable du Sous-traitant, le respect d'une instruction du Responsable devait constituer une violation de la Législation sur la Protection des Données Applicable, le Sous-traitant en informe immédiatement le Responsable par écrit.

3. Confidentialité

3.1. Le Sous-traitant traite les Données Personnelles de manière strictement confidentielle. Le Sous-traitant ne peut divulguer les Données Personnelles à personne d'autre qu'à ses Représentants ou dans la mesure requise par une disposition de la loi applicable.

3.2. Le Sous-traitant ne peut divulguer les Données personnelles aux Représentants que s'ils sont soumis à des obligations strictes de confidentialité et de protection des données qui ne sont pas moins contraignantes que celles imposées au Sous-traitant en vertu de l'Annexe de Traitement des Données.

3.3. Le Sous-traitant doit notifier au préalable par écrit le Responsable de toute divulgation des Données Personnelles que le Sous-traitant ou tout Sous-traitant Approuvé est tenu réaliser en vertu de la loi applicable immédiatement après avoir eu connaissance de cette exigence (à moins que cette notification lui soit interdite par la loi applicable pour des motifs importants d'intérêt public) de manière à offrir au Responsable la possibilité de s'opposer à une telle divulgation.

4. Sécurité

4.1. 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, dont le degré de probabilité et de gravité varie, pour les droits et libertés des Personnes Concernées, le Sous-traitant met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque posé par le traitement des Données Personnelles, en ce compris, le cas échéant :

- 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.

4.2. Le Sous-traitant prend en compte les risques de survenance d'Incidents de Sécurité pour évaluer le niveau de sécurité approprié.

5. Notification d'Incidents de Sécurité

5.1. Le Sous-traitant informe le Responsable par un avis écrit dans les meilleurs délais après avoir eu connaissance de la survenance d'un Incident de Sécurité.

5.2. L'avis écrit relatif à l'Incident de Sécurité contient au moins les informations suivantes :

- une description raisonnablement détaillée de la nature de l'Incident de Sécurité ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre représentant du Sous-traitant pouvant fournir des informations supplémentaires sur l'Incident de Sécurité ;
- les catégories de Données Personnelles affectées par l'Incident de Sécurité ;
- les conséquences probables de l'Incident de Sécurité ; et
- les mesures prises et proposées par le Sous-traitant.

5.3. Le Sous-traitant collabore raisonnablement avec le Responsable dans la gestion de l'Incident de Sécurité.

6. Sous-traitance

6.1. Le Responsable donne son autorisation générale au Sous-traitant de confier la sous-traitance de certaines Données Personnelles aux sous-traitants de second rang repris à l'annexe 2 et aux sous-traitants de second rang ultérieurs ajoutés ou remplacés par le Sous-traitant de temps en temps (les « **Sous-traitants Approuvés** »).

6.2. Le Sous-traitant informe le Responsable de tout changement prévu concernant l'ajout ou le remplacement des sous-traitants de second rang, donnant ainsi au Responsable la possibilité d'émettre des objections à l'encontre de ces changements.

6.3. Le Sous-traitant demeure responsable des actes et omissions des Sous-traitants Approuvés aussi pleinement que s'ils étaient les actes et omissions du Sous-traitant.

6.4. Le Sous-traitant veille à ce que les Sous-traitants Approuvés soient et restent liés par des conditions de traitement des données écrites énonçant des obligations non moins contraignantes que celles prévues dans l'Annexe de Traitement des Données.

7. Transferts transfrontaliers de Données Personnelles

7.1. Le Sous-traitant ne peut pas transférer des Données Personnelles vers un Pays Tiers, à moins que :

- le transfert entre dans le champ d'application d'une décision d'adéquation de la Commission européenne concernant ce Pays Tiers conformément à la Législation sur la Protection des Données Applicable ;
- le transfert entre dans le champ d'application du programme EU-US Privacy Shield et le destinataire des Données Personnelles est certifié sous le programme EU-US Privacy Shield ; ou
- le destinataire des Données Personnelles a conclu avec le Responsable un contrat contenant les clauses types de protection des données approuvées par la Commission européenne ou une autre autorité publique compétente conformément à la Législation sur la Protection des Données Applicable (dans la stricte mesure nécessaire, le Responsable donne mandat au Sous-traitant de conclure un tel contrat avec ledit destinataire au nom et pour le compte du Responsable).

7.2. Si, le cas échéant, le Sous-traitant devait traiter les Données Personnelles depuis un Pays Tiers, le Sous-traitant garantit qu'il fournit des garanties appropriées par rapport à ce transfert conformément à l'article 46 du RGPD.

8. Audit

8.1. À la demande du Responsable, le Sous-traitant met à disposition du Responsable toute information nécessaire pour démontrer la conformité du Sous-traitant à l'Annexe de Traitement des Données et à la Législation sur la Protection des Données Applicable et permet et contribue à des audits, en ce compris des inspections, réalisés par le Responsable ou par un autre auditeur mandaté par le Responsable.

9. Assistance

9.1. Le Sous-traitant collabore avec le Responsable concernant le traitement de demandes de la part des Personnes Concernées relatives à l'exercice de leurs droits en vertu de la Législation sur la Protection des Données Applicable.

9.2. Le Sous-traitant collabore avec le Responsable lors de la conduite d'analyses d'impact à la protection des données à caractère personnel liées à la fourniture du Service.

10. Renvoi/destruction des Données Personnelles

10.1. Dans les trente (30) jours suivant la fin (pour quelque raison que ce soit) de la Convention, le Sous-traitant doit, au choix du Responsable, et moyennant sa demande écrite expresse :

- renvoyer au Responsable dans un format couramment lisible par une machine toutes les Données Personnelles qui, à la date de fin de la Convention, sont en la possession du Sous-traitant ; ou
- détruire toutes les Données Personnelles qui, à la date de fin de la Convention, sont en la possession du Sous-traitant.

10.2. Les obligations relatives au renvoi et à la destruction de Données Personnelles ne s'appliquent pas au Sous-traitant pour les Données Personnels que le Sous-traitant est le cas échéant tenu par la loi applicable de conserver après la fin de la Convention, auquel cas :

- les dispositions de l'Annexe de Traitement des Données survivront à la fin de la Convention et continueront à s'appliquer à ces Données Personnelles ; et
- le Sous-traitant devra, à la demande écrite et expresse du Responsable, s'acquitter de ses obligations de renvoi ou de destruction des Données Personnelles promptement dès que le Sous-traitant n'est plus obligé de conserver ces Données Personnelles.

Annexe 1 : Description du traitement des données

Les catégories de Données Personnelles qui peuvent être accédées/traitées par le Sous-traitant sont les suivantes et concernent les Personnes Concernées suivantes :

- les données d'identification personnelle et professionnelles et les données de contact des représentants des clients du Responsable ;
- les données d'identification personnelle et autres données pertinentes des utilisateurs des produits et/ou des services du Responsable.

Le Sous-traitant traitera les Données Personnelles uniquement dans le cadre des finalités nécessaires à l'accomplissement du Service et pour la durée nécessaire à l'accomplissement du Service.

Annexe 2 : Sous-traitants Approuvés

Entité légale	**Adresse**	**Description du service**
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy L-1855, Luxembourg	Services d'hébergement cloud
Rizq SCS	Avenue Fonsny 46, 1060 Bruxelles, Belgique	Services de développement et maintenance informatique

Abrumet ASBL (Réseau de Santé Bruxellois)	Rue de la Montagne 11, 1000 Bruxelles	Plateforme publique d'échanges de données de santé informatisées