Accord complémentaire concernant le traitement des données de mandat pour le compte du Client

entre

_____

(« **Client** »)

et

Brainlab Sales GmbH, Olof-Palme-Straße 9, 81829 Munich, Germany
(« **Prestataire** », dénommés ensemble les « **Parties contractantes** »)

Préambule

Le présent accord s'applique aux activités du Prestataire liées à l'installation de matériel et de logiciel, à la maintenance, la réparation, la formation, l'accès distant, le dépannage et autres opérations de service après-vente sur les produits du Prestataire, qui aident le Client lors de la fourniture de services de santé et pour lesquels les collaborateurs du Prestataire et les tiers qu'il mandate sont susceptibles d'être en contact avec les données personnelles du Client. L'accord relatif à ces activités ou services est dénommé ci-après contrat principal.

Le présent accord complémentaire est passé en conformité avec le contrat principal et s'aligne sur la durée de celui-ci.

1. Définitions

Dans le présent accord, les termes énumérés ci-dessous ont la signification suivante :

« Pays tiers offrant un niveau de protection des données adéquat » se réfère à tout pays situé en dehors de l'EEE, identifié par la Commission européenne pour offrir, en raison de sa législation nationale ou des obligations internationales qu'il a contractées, un niveau de protection des données adéquat ;

« RGPD » est 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 (règlement général sur la protection des données) ;

« Instruction » est l'ordre écrit du Client axé sur un certain traitement conforme des données personnelles (par exemple l'anonymisation, le blocage, la suppression et la publication) de la part du Prestataire.

Les termes **« Données à caractère personnel », « responsable du traitement », « sous-traitant », « traitement/traiter », « personne concernée », « mesures techniques et organisationnelles », « autorité de contrôle »** ou **« traitement pour le compte d'un responsable du traitement »** doivent être interprétés tels que définis par le RGPD.

2. Objet et responsabilité

Le Prestataire traite des données à caractère personnel pour le compte du Client. L'objet du mandat concerne les activités précisées dans le contrat principal et ses annexes, en particulier dans le cahier des charges. Dans le cadre de cet accord complémentaire, le Client est seul responsable du respect des lois sur la protection des données, en particulier de la légalité de la transmission des données au Prestataire ainsi que de la légalité du traitement des données par le Prestataire.

3. Spécification du contenu du mandat

3.1 Le but, le type et la portée de la collecte, du traitement et/ou de l'utilisation des données à caractère personnel dans le cadre du mandat sont spécifiés dans le contrat principal auquel il est ici fait référence.

3.2 Les types de catégories des données à caractère personnel collectées et/ou utilisées ainsi que les catégories des personnes concernées par la gestion des données personnelles dans le cadre du présent contrat sont décrits à l'annexe 1 et/ou dans le contrat principal auquel il est ici fait référence.

4. Droits d'instruction du Client

4.1 Le Client se réserve, dans le cadre de la spécification visée dans le présent accord, le droit de donner des instructions sur le type, la portée et le processus de traitement des données, qu'il peut préciser par des instructions individuelles. Les modifications apportées à l'objet du traitement et celles apportées aux procédures doivent, quant à elles, être décidées en commun et documentées.

4.2 Le Prestataire informera le Client s'il est d'avis qu'une instruction contrevient aux exigences légales en matière de protection des données. Il est autorisé à suspendre l'exécution de l'instruction tant qu'elle n'a pas été confirmée ou modifiée par le Client.

5. Obligations du Prestataire

5.1 Sauf si la loi ou toute autre disposition le permet (p. ex. consentement de la personne concernée), le Prestataire ne collecte, traite et utilise de manière générale des données que pour le compte du Client et dans le respect des instructions de celui-ci, mais surtout pas à des fins personnelles. Le Prestataire corrigera, supprimera, rectifiera ou bloquera des données à caractère personnel qu'il traite pour le compte du Client uniquement sur instruction de ce dernier. Si une personne concernée s'adresse directement au Prestataire pour faire rectifier ou effacer ses données, celui-ci transmettra la demande au Client.

5.2 Le Prestataire a le droit, dans certains cas, d'utiliser les données qu'il recueille pour le support technique sous une forme qui ne permet pas à ses collaborateurs de tirer des conclusions sur la personne concernée (p. ex. patient, médecin ou personnel hospitalier). Ces données sont utilisées pour (i) satisfaire aux obligations légales (p. ex. obligations de suivi des produits et obligations de déclaration) ou pour (ii) préserver les intérêts justifiés du Prestataire et du Client, en particulier améliorer la qualité et la fonctionnalité des produits du Prestataire par l'utilisation de données de support sélectionnées (p. ex. photos dépersonnalisées de scanner ou IRM) en vue de tester notamment de nouvelles versions de produits. Les autres restrictions contenues dans le présent accord pour le traitement des données à caractère personnel dans le cadre du mandat ne s'appliquent pas ici.

5.3 Les données sont traitées uniquement sur instruction du Client, à moins que le Prestataire ne soit tenu d'y procéder en vertu de la législation de l'Union européenne ou de l'État membre à laquelle il est soumis. Dans ce cas, le Prestataire informe le Client de cette

obligation juridique avant le traitement, sauf si la législation concernée interdit une telle information pour des motifs importants d'intérêt public (cf. art. 28, al. 3 lettre a RGPD).

5.4 Sauf interdiction par les dispositions légales en vigueur ou sur demande des autorités, le Prestataire doit immédiatement informer le Client de toutes les demandes émanant des organismes d'État, des autorités chargées de la protection des données ou des autorités judiciaires concernant l'accès ou la saisie des données à caractère personnel du Client.

5.5 Avant l'octroi de l'accès aux données à caractère personnel, le Prestataire obligera les personnes chargées du traitement des données à caractère personnel à respecter le secret et la confidentialité des données et les initiera aux modalités des obligations en vigueur pour le Prestataire. L'obligation pour les personnes concernées de respecter un éventuel secret professionnel (dérivé), par exemple pour le traitement de données émanant d'hôpitaux ou de médecins établis, ou la confidentialité des télécommunications en fait partie si nécessaire, si et dans la mesure où il a été convenu de prestations appropriées dans le contrat principal. Dans la mesure requise par le droit professionnel et la déontologie, le Client prendra toutes les mesures requises, puis informera et instruira le Prestataire.

5.6 Dans la mesure où le droit l'exige, le Prestataire désigne un délégué à la protection des données et met les coordonnées de celui-ci à disposition du Client pendant la durée du contrat principal.

5.7 Le Prestataire informera le Client des violations, de sa part ou de la part d'une personne qu'il emploie, d'instructions ou de dispositions sur la protection des données personnelles du Client.

S'il y a perte, transmission illégale ou divulgation à des tiers de toute autre manière illicite selon les arts. 33 et 34 du RGPD de données à caractère personnel, le Client doit en être informé immédiatement. En accord avec le Client, le Prestataire prend des mesures appropriées afin de protéger les données et d'atténuer les éventuelles conséquences négatives pour les personnes concernées.

De plus, il avisera immédiatement le Client des dysfonctionnements majeurs intervenant dans le fonctionnement normal, de toute suspicion de violations de la protection des données ou de toute autre irrégularité dans le traitement des données à caractère personnel.

Le Prestataire est au courant que le Client est tenu de documenter les violations de données à caractère personnel et, le cas échéant, d'informer l'autorité de contrôle ou la personne concernée d'une telle violation. Si et dans la mesure où de telles violations se sont produites, le Prestataire aide le Client conformément à l'art. 28 al. 3 lettre f RGPD à s'acquitter de ses obligations de manière appropriée afin que celui-ci puisse les remplir dans les délais. Le Prestataire notifiera la violation au Client et formulera au moins les données suivantes pour autant qu'il reçoit des informations adéquates :

a) une description de la nature de la violation de la protection des données à caractère personnel, si possible avec mention des catégories et du nombre approximatif de personnes concernées, des catégories concernées et du nombre approximatif de jeux de données personnelles concernés.

b) le nom et les coordonnées du délégué à la protection des données ou d'un autre contact afin d'obtenir de plus amples informations ;

c) une description des conséquences probables de la violation des données à caractère personnel ;

d) une description des mesures prises ou proposées par le Client pour remédier à cette violation et, le cas échéant, des mesures visant à atténuer ses éventuelles conséquences négatives.

5.8 Le Prestataire informe immédiatement le Client de toutes les activités de surveillance et des mesures qui ont été prises par l'autorité de contrôle en lien avec le traitement de ses données à caractère personnel.

5.9 Si, conformément aux dispositions légales de protection des données en vigueur, le Client est tenu d'informer sur la collecte, le traitement ou l'utilisation des données, le Prestataire doit mettre toutes les informations appropriées à disposition du Client.

5.10 Pendant l'exécution du traitement des données demandé, le Prestataire veille au respect des obligations mentionnées ci-dessus.

5.11 Le Prestataire tient un registre écrit de toutes les catégories d'activités de traitement en vertu de l'art. 30 al. 2 RGPD, effectuées pour le compte du Client.

5.12 Le cas échéant, le Prestataire aide conformément à l'art. 28 al. 3 lettre f RGPD à l'établissement d'une analyse d'impact relative à la protection des données selon l'art. 35 RGPD et apporte son assistance, lorsque cela s'avère utile, lors de la consultation préalable de l'autorité de contrôle conformément à l'art 36 RGPD. Le Prestataire doit remettre au Client les informations et les dossiers requis si ce dernier les lui demande. Les frais supplémentaires découlant de ces prestations doivent être remboursés au Prestataire.

5.13 Le Prestataire prend des mesures appropriées concernant l'utilisation abusive, la perte et la restauration des données (p. ex. en effectuant des sauvegardes selon la norme industrielle) pour autant que cela soit prévu dans le contrat principal.

6. Sécurité du traitement des données

6.1 Dans les limites de sa compétence, le Prestataire met en place son organisation interne en fonction des exigences de protection et de sécurité des données en vigueur. Il prend, gère et contrôle des mesures techniques et organisationnelles afin d'assurer une protection adéquate des données du Client contre toute utilisation abusive et perte, et ce en conformité avec les lois en vigueur.

6.2 Le Prestataire prend toutes les mesures techniques et organisationnelles appropriées conformes aux exigences de l'art. 32 RGPD afin de garantir un niveau de protection adapté au risque et d'aider le Client à respecter les obligations visées à l'art. 32 RGPD (art. 28 al. 3 lettres c et f RGPD).

6.3 Dans ce cadre, le Prestataire tient compte de l'état de la technique, des coûts de mise en œuvre, du type, de la portée, du contexte et des finalités du traitement ainsi que du risque, dont le degré de probabilité et de gravité varie, pour les droits et les libertés des personnes physiques. Des mesures appropriées telles que le contrôle initial, le contrôle des utilisateurs, le contrôle des accès, le contrôle de la transmission, le contrôle de la saisie, le contrôle des mandats, le contrôle de la disponibilité et la séparation selon l'objet font partie de ce cadre, de même que :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) la capacité à garantir sur la durée la confidentialité, l'intégralité, la disponibilité et la résilience des systèmes et des services liés au traitement ;

c) la capacité à rétablir rapidement la disponibilité des données à caractère personnel et l'accès à ces données en cas d'incident physique ou technique ;

d) une opération de vérification et d'évaluation régulières de l'efficacité des mesures techniques et organisationnelles en vue d'assurer la sécurité du traitement.

6.4 L'annexe 2 contient une description et une spécification des mesures techniques et organisationnelles requises que le Prestataire effectuera dans le cadre du présent accord. Elles peuvent être complétées par d'autres documents.

6.5 Les mesures techniques et organisationnelles évoluent en fonction des progrès techniques et du développement. Le Prestataire peut prendre des mesures alternatives appropriées. Celles-ci ne doivent cependant pas présenter un niveau de sécurité inférieur aux mesures fixées. Les modifications essentielles doivent être documentées.

6.6 Conformément à l'art. 28 al. 3 lettre e, le Prestataire aide le Client par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation visée à l'alinéa 3 RGPD à l'égard des personnes concernées pour ce qui a trait à, par exemple, l'information des personnes concernées, leur droit d'accès aux données, la rectification et la suppression des données, la limitation du traitement ou du droit à la portabilité des données et au droit de contestation. Les frais supplémentaires découlant de ces prestations doivent être remboursés au Prestataire.

7 Accès distant et accès au support technique

7.1 Les règlements suivants s'appliquent à titre complémentaire pour l'exécution des accès distant et accès au support technique, si et dans la mesure où les activités de traitement concernent des catégories particulières de données personnelles ou si le Client est soumis à un secret professionnel.

7.2 Dans la mesure où un accès aux données à caractère personnel ne peut être exclu, les accès distants sont réalisés exclusivement avec l'accord des collaborateurs compétents du Client.

7.3 Les collaborateurs du Client utilisent des méthodes d'identification et de chiffrement appropriées.

7.4 Les accès distants sont documentés et enregistrés. Le Client est autorisé à contrôler les tâches de vérification et de maintenance avant, pendant et après l'exécution. Il doit pour ce faire respecter les dispositions évoquées à l'alinéa 9. Concernant les accès distants, le Client est, dans la mesure où cela est techniquement possible et réalisable vu le type de prestations fournies, autorisé à suivre ces prestations depuis un écran de contrôle et à les interrompre à tout moment.

7.5 Les accès distants aux systèmes importants obéissent uniquement au principe du « need to know ».

7.6 Les opérations d'analyse d'erreurs qui requièrent un accès aux données personnelles doivent être approuvées au préalable par les collaborateurs compétents du Client. Si des copies sont effectuées à ces fins, le Prestataire les modifiera après rectification de l'erreur afin de supprimer tout lien avec les personnes ou les détruira, à moins que la conservation (inchangée) des données correspondantes ne soit exigée pour d'autres raisons (p. ex. preuve des tâches réalisées et de leur conformité). Les données à caractère personnel ne peuvent être utilisées qu'à des fins d'analyse d'erreur et ne peuvent être copiées sur des supports de données mobiles (PDA, clés USB ou périphériques similaires) sans chiffrement approprié. Le point 5.2 reste inchangé.

7.7 Il est possible dans certains cas que les tâches d'analyse d'erreurs soient effectuées sans demande de consentement préalable, si cela est indispensable pour la fourniture des prestations contractuelles (notamment à des fins de remise en état). Le Client donne ici un accord général pour des actions appropriées.

7.8 Les accès distants et l'ensemble des activités requises dans ce cadre, en particulier la suppression, le transfert de données ou l'analyse d'erreurs, sont effectués en tenant compte des mesures techniques et organisationnelles pour la protection de données à caractère personnel.

8. Droits et obligations du Client

8.1 Le Client et le Prestataire sont responsables du respect des législations pertinentes de protection en ce qui concerne les données à traiter.

8.2 Le Client fixe les mesures de restitution des supports de données cédés et/ou de suppression des données sauvegardées à la fin du mandat. En l'absence de telles décisions, les données doivent être remises au Client ou supprimées. Si les données sont supprimées à la suite de décisions particulières, la suppression doit être confirmée par le

Prestataire au Client en mentionnant la date. Il n'est possible de restituer ou d'effacer les données sauvegardées que s'il n'y a aucune obligation légale ou réglementaire de conservation à laquelle serait soumis le Prestataire. Le point 5.2 reste inchangé.

9. Droits de contrôle

9.1 Sur demande du Client, le Prestataire met à sa disposition des preuves justificatives de la mise en œuvre des mesures techniques et organisationnelles ainsi que des autres obligations conformément à l'art. 28 RGPD.

9.2 En accord avec le Prestataire, le Client peut effectuer un contrôle du mandat ou charger un auditeur de le faire avant le début du traitement des données ou de façon raisonnable pendant toute la durée du mandat. Le Prestataire peut satisfaire à ces exigences à tout moment avant le début et pendant la durée du traitement par des auto-évaluations appropriées, des certificats en vigueur, des comptes rendus ou des extraits de rapports d'organismes indépendants (auditeurs externes, audits internes, délégué à la protection des données, département de sécurité informatique, contrôleur de la protection des données ou contrôleur de la qualité) ou par une certification appropriée dans le cadre d'un audit de sécurité informatique ou audit de protection de données personnelles.

9.3 Si le Client a des doutes justifiés à exposer au Prestataire sur l'auto-évaluation ou l'évaluation présentée par ce dernier, il est même autorisé à mener à ses frais un audit approprié dans les locaux commerciaux du Prestataire afin de vérifier le respect des mesures techniques et organisationnelles et le reste des obligations visées à l'art. 28 RGPD. Un audit de ce genre doit être notifié au moins deux semaines à l'avance. Il peut être mené uniquement pendant les heures de bureau réglementaires et ne doit pas perturber le fonctionnement interne. Le Client doit rembourser tous les frais supplémentaires encourus par le Prestataire par un audit approprié.

9.4 Sur demande écrite du Client, le Prestataire met à sa disposition dans un délai adapté les informations et les documents requis pour l'audit.

10. Sous-traitants

10.1 Le Prestataire est autorisé à mandater des sous-traitants et d'autres entreprises pour l'exécution de leurs obligations contractuelles.

10.2 Par la conclusion d'accords avec les sous-traitants, le Prestataire s'assure qu'ils aient, du moins pour l'essentiel, les mêmes obligations que lui-même conformément à l'accord complémentaire, avant que l'accès aux données à caractère personnel du Client soit octroyé au sous-traitant pendant l'exécution. Si le sous-traitant fournit la prestation convenue en dehors de l'UE/l'EEE et d'un pays tiers ayant un niveau de protection de données approprié, le Prestataire veille au respect de la politique de confidentialité de l'UE par des mesures adéquates.

10.3 Sur demande, le Prestataire met à disposition une liste des sous-traitants participant aux activités de traitement des données réalisées ci-après. Il informe le Client de toutes les modifications envisagées concernant l'ajout ou le remplacement d'autres sous-traitants, et lui donne ainsi la possibilité de refuser ces modifications, tout en formulant une objection fondée. Si le Client refuse un nouveau sous-traitant, le Client et/ou le Prestataire peut résilier par écrit sans préavis, c'est-à-dire sans respecter le délai, les services concernés par le traitement, pour lequel le sous-traitant doit être consulté, ainsi que toute autre obligation d'indemnités de dommages et intérêts et de frais.

10.4 Le Client est autorisé à contrôler les sous-traitants du Prestataire conformément au point 9 et après discussion et accord avec le Prestataire. Le Client charge ici le Prestataire d'effectuer le contrôle pour son compte et est d'accord pour qu'un tel audit ne soit réalisé que par le Prestataire, mais également sur présentation de certificats en vigueur, comptes rendus ou extraits de rapports d'organismes indépendants (auditeurs externes, audits internes, délégué à la protection des données, département de sécurité informatique,

contrôleur de la protection des données ou contrôleur de la qualité) ou par une certification appropriée dans le cadre d'un audit de sécurité informatique ou audit de protection de données personnelles. Avant la transmission des documents et des informations appropriés du sous-traitant, le Client doit le cas échéant signer un ou plusieurs accords de confidentialité avec le sous-traitant et/ou le Prestataire.

10.5 Les consignes visées au point 10 ne s'appliquent pas si le Prestataire confie des prestations annexes à des tiers. Celles-ci incluent entre autres les services de poste, d'expédition et de facility management.

11. Transferts de données en dehors de l'EEE

11.1 En règle générale, le traitement des données est effectué dans un État membre de l'Union européenne, un pays de l'Espace économique européen ou un pays tiers affichant un niveau de protection adéquat (y compris les États-Unis, pour autant qu'une certification de protection des données personnelles existe)**.** Les traitements dans un autre pays (« **pays tiers** ») sont licites si les exigences en vigueur pour la transmission internationale de données à caractère personnel conformément à l'art. 44 ss. RGPD sont respectées.

11.2 Si et dans la mesure où (i) le Client et le Prestataire sont situés dans l'Espace économique européen (« **EEE** »), tandis que le sous-traitant du Prestataire est situé dans un pays tiers et où (ii) le Prestataire conclut des accords avec des sous-traitants sur la base des clauses contractuelles types de l'UE pour Prestataires (« **SCC** »), le Client autorise par là même le Prestataire à signer des accords de traitement avec des sous-traitants en son nom et pour son compte, pour autant que celui-ci le puisse. Si exigé, le Prestataire doit informer le Client et les Parties contractantes de l'existence et de l'état des clauses contractuelles types passées dans les circonstances précitées. Il appartient au Prestataire d'évaluer si des contrats appropriés sont conclus.

12. Responsabilité

12.1 Le Client libère le Prestataire de toute exigence de tiers ou d'autres préjudices et obligations découlant de (i) la violation des obligations du Client issues de cet accord et/ou d'autres infractions aux législations de protection des données en vigueur, et/ou des (ii) infractions du Prestataire aux législations de protection des données en vigueur, dans la mesure où celles-ci sont fondées sur l'exécution des décisions du présent contrat ou d'autres instructions du Client. Cette clause ne s'applique pas si le Client n'est pas responsable des circonstances engageant la responsabilité. L'art. 82 (5) RGPD reste inchangé.

12.2 Dans la mesure où le contrat principal prévoit une limitation ou une exclusion de la responsabilité ou une obligation d'exonération du Prestataire, ces restrictions ou exclusions s'appliquent aussi aux réclamations à l'encontre du Prestataire dans le cadre du présent accord complémentaire.

12.3 Les dispositions du contrat principal relatives à la responsabilité ou à l'exonération restent inchangées à tous autres égards.

13. Confidentialité

Les Parties contractantes s'engagent à traiter de manière confidentielle tous les éléments de connaissance sur les secrets commerciaux et industriels obtenus dans le cadre du rapport contractuel. La confidentialité s'applique également au-delà du terme des mandats et/ou de la relation commerciale.

14. Obligations d'information, clause requérant la forme écrite, droit applicable

14.1 Si les données à caractère personnel du Client sont mises en danger chez le Prestataire en raison d'une saisie ou d'une mise sous séquestre, d'une procédure d'insolvabilité ou de concordat ou d'autres événements ou interventions de tiers, le Prestataire est tenu d'en informer immédiatement le Client.

Il informera toutes les Parties contractantes que la souveraineté et la propriété des données relèvent exclusivement du Client.

14.2 Les modifications et les compléments au présent accord complémentaire requièrent la forme écrite et une référence expresse au fait qu'il s'agit d'une modification ou d'un complément à l'accord. Toute modification de cette exigence formelle requiert la forme écrite.

14.3 Le présent accord complémentaire et tous les litiges liés à sa conclusion et son exécution sont régis exclusivement par la législation de la République fédérale d'Allemagne, à l'exclusion de la Convention de Vienne des Nations Unies du 11 avril 1980 sur les contrats de vente internationale de marchandises. Le tribunal compétent pour les litiges susceptibles de survenir entre les Parties dans le cadre de cet accord complémentaire est le tribunal régional (Landgericht) de Munich I.

Pour le Prestataire :	**Pour le Client :**
[*Nom*] [Fonction] [*Lieu, date*]	[*Nom]* [Fonction] [*Lieu, date*]
_____	_____

<u>Annexe 1</u> : Types de catégories de données et catégories de personnes concernées dans le cadre de la collecte, du traitement et/ou de l'utilisation des données à caractère personnel

1. Types de données collectées et/ou de données à caractère personnel utilisées

- Données de base des personnes (p. ex. prénom, nom, date de naissance, sexe, ID du patient)
- Coordonnées (p. ex. téléphone, e-mail)
- Données de base du contrat (p. ex. relation contractuelle, intérêt pour les produits ou les contrats)
- Historique du Client
- Données de facturation et de paiement (p. ex. numéro de compte bancaire)
- Données de planification et de gestion (p. ex. informations sur l'infrastructure client)
- Données d'évaluation (de tiers, p. ex. agences de notation, ou de registres publics)
- Informations médicales et photos des patients

2. Catégories de personnes soumises au traitement des données à caractère personnel

- Clients
- Clients potentiels
- Abonnés
- Patients du Client

<u>Annexe 2</u> : Sécurité du traitement des données

Cette annexe décrit les mesures techniques et opérationnelles (MTO) et les procédures que le Prestataire doit respecter a minima afin de préserver la sécurité des données à caractère personnel créées, collectées, reçues ou obtenues autrement et de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

Mesures techniques et organisationnelles

I. Confidentialité, art. 32 al. 1 lettre b RGPD

1. Contrôle des accès

Mesures permettant de refuser aux personnes non autorisées l'accès aux systèmes traitant ou utilisant les données à caractère personnel.

- ☒ Définition d'un groupe limité de personnes disposant d'une autorisation d'entrée
- ☒ Serrures de sécurité
- ☒ Système de fermeture manuel (p. ex. pièce verrouillable, armoire) - applicable spécifiquement pour le bureau à domicile
- ☒ Système de fermeture à carte à puce/à transpondeur
- ☒ Surveillance vidéo des accès

2. Contrôle de l'accès aux données

Mesures permettant d'interdire que les systèmes de traitement des données soient utilisés par des personnes non autorisées.

- ☒ Attribution fonctionnelle et/ou limitée dans le temps des autorisations utilisateurs
- ☒ Règle de mot de passe, incluant la longueur, l'attribution et le changement de mot de passe
- ☒ Authentification par nom d'utilisateur/mot de passe
- ☒ Utilisation de détecteurs d'intrusion et de systèmes de prévention des intrusions
- ☒ Utilisation de logiciel antivirus
- ☒ Utilisation d'un pare-feu matériel
- ☒ Utilisation de filtres antispam
- ☒ Création de profils utilisateurs
- ☒ Affectation de profils utilisateurs aux systèmes informatiques
- ☒ Utilisation de la technologie VPN
- ☒ Utilisation de logiciel centralisé de gestion des smartphones (p. ex. pour la suppression externe des données)
- ☒ Utilisation d'un pare-feu logiciel
- ☒ Cryptage du disque dur pour les ordinateurs portables
- ☒ Système de connexion supplémentaire pour différentes applications

3. Contrôle des supports de stockage

Mesures garantissant que les personnes autorisées à utiliser un système de traitement des données accèdent exclusivement aux données soumises à leur autorisation d'accès et que les données à caractère personnel ne soient pas lues, copiées, modifiées, ni supprimées lors de leur traitement, de leur utilisation et après leur sauvegarde.

- ☒ Définition des autorisations d'accès
- ☒ Attribution restrictive des autorisations d'administration
- ☒ Effacement physique des supports de données avant réutilisation
- ☒ Enregistrement des transferts de données
- ☒ Nécessité de l'identification du mot de passe
- ☒ Administration des droits par l'administrateur du système
- ☒ Stockage sécurisé des supports de données
- ☒ Enregistrement des accès sur différentes applications
- ☒ Processus définis pour l'octroi des autorisations, le contrôle et le retrait des autorisations
- ☒ Destruction sécurisée des supports de données

4. Contrôle de la séparation

Mesures garantissant que les données collectées à différentes fins font l'objet d'un traitement séparé.

- ☒ Sauvegarde physiquement séparée sur des systèmes ou des supports de données distincts
- ☒ Création d'un concept d'autorisation
- ☒ Différentiation logique des mandants (au niveau du logiciel)
- ☒ Séparation entre le système productif et le système de test

II. Pseudonymisation et chiffrement, art. 32 al. 1 lettre a RGPD

Mesures de pseudonymisation et de chiffrement des données à caractère personnel (dans la mesure où elles ne sont pas visées au point 1)

- ☒ Utilisation de techniques de pseudonymisation et d'anonymisation, notamment dans le domaine R&D
- ☒ Existence de règles pour le chiffrement des données
- ☒ Chiffrement de données particulièrement sensibles (« at rest ») dans tous les services

III. Intégrité, art. 32 al. 1 lettre b RGPD

1. Contrôle du transfert de données

Mesures garantissant que des données à caractère personnel soient, lors de la transmission électronique, de leur transport ou de leur stockage sur des supports de données, lues, copiées, modifiées ou supprimées de manière illicite et que soit vérifié et constaté à quelles instances des données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données.

- ☒ Installations de lignes dédiées ou tunnels VPN
- ☒ Formation des collaborateurs en matière de protection des données
- ☒ Documentation des destinataires des données
- ☒ Une directive établit clairement l'attitude à adopter en cas de perte de support de données.
- ☒ Cryptage du disque dur pour les ordinateurs portables

2. Contrôle de la saisie

Mesures garantissant que l'on puisse vérifier et constater a posteriori si des données à caractère personnel ont été saisies, modifiées et supprimées dans les systèmes de traitement de données et par qui.

- ☒ Attribution de droits de saisie, modification et suppression de données sur la base d'un concept d'autorisation
- ☒ Enregistrement de la saisie, de la modification et de la suppression de données, dans la mesure où les systèmes le permettent.

IV. Disponibilité et résilience, art. 32 al. 1 lettre b et c RGPD

1. Contrôle de la disponibilité

Mesures garantissant que des données à caractère personnel soient protégées contre toute destruction fortuite ou perte fortuite, y compris des mesures de restauration en cas d'incidents physiques ou techniques.

- ☒ Alimentation sans coupure (ASC)
- ☒ Contrôle climatique dans les salles de serveurs
- ☒ Détecteurs d'incendie et de fumée
- ☒ Système de sauvegarde et de restauration
- ☒ Existence d'un plan d'urgence
- ☒ Utilisation de pare-feux et de scanners antivirus
- ☒ Gestion des correctifs
- ☒ Système anti-incendie adapté dans les salles de serveurs
- ☒ Test de récupération des données
- ☒ Stockage de sauvegarde en lieu sécurisé et délocalisé

V. Procédure visant à analyser et à évaluer régulièrement l'efficacité des mesures, art. 32 al. 1 lettre d RGPD

1. Gestion de la protection des données

Autres mesures, notamment mesures organisationnelles de protection des données à caractère personnel.

- ☒ Description des consignes de protection actuelles dans des directives et des instructions contraignantes.
- ☒ Collecte d'informations actuelles relatives à la sécurité informatique et aux failles de sécurité.
- ☒ Vérifications régulières des préparatifs concernant la protection des données et des règles actuelles
- ☒ Le cas échéant, intégration du délégué à la protection des données dans de nouvelles procédures de traitement des données pertinentes.

2. Gestion des incidents de sécurité

Autres mesures de gestion des incidents liés à la protection des données

- ☒ Règles de conduite en cas d'incidents liés à la protection des données et à la sécurité informatique
- ☒ Processus de gestion de la continuité des affaires
- ☒ Processus de signalement des incidents

3. Protection des données par défaut, art. 25 al. 2 RGPD

Mesures garantissant que la protection par défaut répond aux intérêts des personnes concernées (privacy by default).

- ☒ Mise en œuvre de la protection des données par défaut
- ☒ Utilisation de la pseudonymisation ou de l'anonymisation des données à caractère personnel, notamment dans le domaine R&D
- ☒ Limitation de la collecte des données

4. Contrôle du mandat

Mesures garantissant que les données à caractère personnel traitées au cours du mandat ne peuvent l'être que conformément aux instructions du Client.

- ☒ Choix du Prestataire selon des critères de précaution (notamment eu égard à la sécurité des données)
- ☒ Contrôle préalable du sous-traitant, en particulier examen préalable de la documentation des mesures de sécurité prises chez le Prestataire
- ☒ Instructions documentées transmises au Prestataire (p. ex. par le contrat de sous-traitance)
- ☒ Obligation du sous-traitant à obliger ses collaborateurs à respecter la confidentialité des données
- ☒ Le Prestataire a, le cas échéant, désigné le délégué à la protection des données.
- ☒ Droits de contrôle efficaces convenus par rapport au Prestataire
- ☒ Formation des collaborateurs
- ☒ Registre des activités de traitement des mandats