xatla AG Logiciels d'entreprise
Dorfmattweg 8a | 3110 Münsingen
+41 31 331 01 01 | info@xatla.ch

Contrat de sous-traitance

1 Objet

Le présent contrat régit les droits et obligations de xatla AG en tant que sous-traitant et du donneur d'ordre, un client de xatla AG (ci-après dénommés conjointement les « parties ») en ce qui concerne le traitement des données à caractère personnel (ci-après dénommées «données à caractère personnel») dans le cadre du traitement des commandes ou du traitement des données (ci-après dénommés de manière uniforme «traitement des commandes») conformément à la législation sur la protection des données.

Par le présent contrat, le prestataire permet au donneur d'ordre de se conformer aux exigences applicables en matière de protection des données pour le traitement des données.

Le présent contrat s'applique à toutes les activités dans le cadre desquelles le prestataire traite, en tout ou en partie, des données à caractère personnel pour le compte du donneur d'ordre ou fait traiter (ci-après dénommé de manière uniforme « traiter ») de telles données.

Le mandataire est soumis au droit suisse de la protection des données, en particulier à la loi fédérale sur la protection des données (LPD). Par décision du 26 juillet 2000, la Commission européenne a constaté que le droit suisse de la protection des données garantissait un niveau de protection adéquat des données à caractère personnel. Cette constatation vaut décision d'adéquation au sens de l'art. 45, al. 1, du règlement général européen sur la protection des données (RGPD).

2 Nature, objet et finalité du traitement des données pour le compte d'autrui

Le traitement des données pour le compte d'un tiers s'effectue conformément aux accords contractuels existants ou à conclure entre les parties, tels que notamment les conditions générales de vente (CGV). Les dispositions du présent contrat prévalent en cas de contradiction entre les dispositions du présent contrat et d'autres accords contractuels entre les parties.

Le traitement des données à caractère personnel comprend toute opération portant sur des données à caractère personnel, quels que soient les moyens et procédures utilisés, notamment la consultation, la comparaison, l'adaptation, l'archivage, la conservation, la lecture, la communication, l'obtention, la limitation, la collecte, la collecte, la suppression, la divulgation, le classement, l'organisation, le stockage, la modification, l'interconnexion, la destruction et l'utilisation de données à caractère personnel. Les données à caractère personnel sont toutes les informations se rapportant à une personne physique identifiée ou identifiable dont les données sont traitées.

Le traitement des données pour le compte d'un tiers porte sur les catégories de données à caractère personnel énumérées **à l'annexe 1**.

Le traitement des données pour le compte d'un tiers comprend les catégories de personnes concernées dont les données à caractère personnel sont traitées, conformément à **l'annexe 2**.

3 Obligations des parties

3.1 Instructions et limitation de la finalité

Le sous-traitant traite les données à caractère personnel exclusivement aux fins prévues dans les accords contractuels entre les parties ou conformément aux instructions documentées du responsable du traitement, sauf si le sous-traitant est légalement ou réglementairement tenu d'effectuer un traitement spécifique. Le responsable du traitement peut donner des instructions documentées supplémentaires pendant toute la durée du traitement.

Le sous-traitant informe le donneur d'ordre s'il ne peut pas exécuter, en tout ou en partie, une instruction qui lui a été donnée. Le sous-traitant informe le donneur d'ordre s'il estime que les accords contractuels ou les instructions données enfreignent les exigences applicables en matière de protection des données.

3.2 Sécurité

Le sous-traitant prend au moins les mesures techniques et organisationnelles (MTO) appropriées conformément **à l'annexe 3** afin de garantir une sécurité des données personnelles traitées (ci-après la «sécurité des données») adaptée au risque. Ces mesures comprennent notamment la protection des données personnelles traitées, y compris, le cas échéant, les données personnelles sensibles, contre toute violation de la sécurité des données.

12 Le mandataire n'accorde à ses auxiliaires l'accès aux données personnelles du mandant que dans la mesure où cet accès est nécessaire à l'exécution, au contrôle et à la gestion du présent contrat. Le mandataire garantit que les personnes habilitées à traiter les données se sont engagées à respecter le secret ou sont soumises à une obligation légale de confidentialité appropriée.

3.3 Documentation et possibilités de contrôle

Les parties doivent être en mesure de prouver le respect du présent contrat.

Le prestataire traite de manière appropriée et dans les meilleurs délais les demandes du donneur d'ordre concernant le traitement des données conformément au présent contrat.

Sur demande, le prestataire met à la disposition du donneur d'ordre toutes les informations disponibles nécessaires pour prouver le respect des exigences fixées dans le présent contrat et découlant directement des dispositions applicables en matière de protection des données.

Le prestataire permet au donneur d'ordre, sur demande, de contrôler le traitement des données conformément au présent contrat à des intervalles raisonnables ou en cas d'indices documentés de non-respect.

Le donneur d'ordre peut effectuer lui-même un tel contrôle ou le faire effectuer par un contrôleur indépendant. Ces contrôles sont limités à un jour par année civile. Un contrôle peut également inclure des inspections dans les installations physiques ou les locaux du sous-traitant, pour autant que ces inspections soient nécessaires, qu'elles aient lieu pendant les heures d'ouverture habituelles sans perturber le déroulement des opérations et que la notification soit effectuée en respectant un délai raisonnable. De telles inspections ne sont par ailleurs autorisées que si et dans la mesure où la vérification ne peut être effectuée à l'aide de preuves appropriées telles que des attestations, des documents et des certificats ou des certifications, en particulier dans le cas des centres de données.

Le donneur d'ordre prend en charge les frais engagés par le prestataire pour ces vérifications.

Les parties mettent les informations susmentionnées, y compris les résultats des contrôles, à la disposition de l'autorité de contrôle compétente ou des autorités de contrôle compétentes sur demande, pour autant que cette mise à disposition ne soit pas interdite pour des raisons légales.

4 Sous-traitance

Le donneur d'ordre accorde au preneur d'ordre l'autorisation générale de faire appel à des sous-traitants figurant sur la liste de **l'annexe 4**.

Le prestataire informe le donneur d'ordre au moins 30 jours à l'avance, par voie électronique ou par écrit, de toute modification envisagée de cette liste par le remplacement ou l'ajout de sous-traitants. Le prestataire accorde ainsi au donneur d'ordre un délai suffisant pour pouvoir soulever d'éventuelles objections aux modifications envisagées avant la passation de la commande.

En l'absence d'opposition dans les délais impartis, les modifications envisagées sont réputées approuvées. Si, en cas d'opposition, les parties ne parviennent pas à trouver un accord sur les modifications prévues et si le donneur d'ordre n'est pas disposé à renoncer à son opposition, les parties sont en droit de résilier le présent contrat de manière extraordinaire à la date prévue pour les modifications.

Le prestataire doit imposer contractuellement aux sous-traitants chargés de l'exécution du traitement des données essentiellement les mêmes obligations que celles qui s'appliquent au prestataire en vertu du présent contrat. Le prestataire veille à ce que chaque sous-traitant respecte les obligations auxquelles le prestataire est soumis en vertu du présent contrat et conformément aux exigences applicables en matière de protection des données.

5 Exportation de données à caractère personnel

Tout transfert de données à caractère personnel vers un pays situé en dehors de la Suisse et des États membres de l'Espace économique européen (EEE) ou vers une organisation internationale s'effectue exclusivement conformément aux dispositions contractuelles ou aux instructions documentées du donneur d'ordre, sauf si le prestataire est légalement tenu de procéder à un tel transfert. Dans un tel cas, le mandataire informe le mandant de cette obligation légale, pour autant qu'une telle information ne soit pas interdite pour des raisons légales.

Tout transfert de données à caractère personnel vers un pays situé en dehors de la Suisse et des États membres de l'EEE n'a lieu, en principe, que si la législation en matière de protection des données du pays concerné garantit, selon le Préposé fédéral à la protection des données et à la transparence (PFPDT) ou le Conseil fédéral suisse, un niveau de protection adéquat des données à caractère personnel.

L'exportation de données personnelles vers un pays situé en dehors de la Suisse et des États membres de l'EEE, dont la législation en matière de protection des données ne garantit pas un niveau de protection adéquat des données personnelles, peut avoir lieu à titre exceptionnel si, pour d'autres raisons, un niveau de protection adéquat est garanti conformément aux exigences applicables en matière de protection des données, notamment en vertu d'accords intergouvernementaux ou sur la base de clauses contractuelles types en vigueur adoptées par la Commission européenne. Le sous-traitant est autorisé à adapter et à compléter ces clauses contractuelles types européennes conformément aux recommandations du PFPDT, de manière à ce que les clauses contractuelles types répondent également aux exigences applicables en matière de protection des données en Suisse et soient ainsi aptes à garantir un niveau de protection adéquat lors de l'exportation de données depuis la Suisse.

Le recours à Nylas Inc., États-Unis, en tant que sous-traitant s'effectue en application des clauses types de protection des données de la Commission européenne, conformément à la recommandation du Préposé fédéral à la protection des données et à la transparence (PFPDT). Une copie des garanties applicables peut être fournie sur demande.

6 Assistance au donneur d'ordre

Le sous-traitant informe sans délai le donneur d'ordre de toute demande relative à la protection des données qu'il a reçue d'une personne concernée et qui concerne le traitement des données. Le sous-traitant est en droit de confirmer la réception de la demande à la personne concernée, mais ne répond pas lui-même à la demande, sauf s'il en a été chargé par le donneur d'ordre.

Le sous-traitant assiste le donneur d'ordre, en tenant compte de la nature du traitement des données, dans l'accomplissement de son obligation de répondre aux demandes des personnes concernées en matière de protection des données.

Le sous-traitant assiste en outre le donneur d'ordre, en tenant compte de la nature du traitement et des informations disponibles, dans le respect des obligations suivantes :

- Tenue d'un éventuel registre des activités de traitement ;
- Réalisation d'une analyse d'impact relative à la protection des données lorsque le traitement prévu de données à caractère personnel par le donneur d'ordre est susceptible d'entraîner un risque élevé pour les droits fondamentaux ou la personnalité des personnes concernées ;
- Consultation de l'autorité ou des autorités de contrôle compétentes avant le traitement de données à caractère personnel, si une analyse d'impact relative à la protection des données révèle que le traitement prévu comporte un risque élevé pour les droits fondamentaux ou la personnalité des personnes concernées, malgré les mesures prévues.

Le donneur d'ordre prend en charge les frais engagés par le prestataire pour cette assistance.

7 Notification des violations de la sécurité des données

En cas de violation de la sécurité des données, le prestataire coopère avec le donneur d'ordre. Le prestataire assiste le donneur d'ordre dans l'exécution de ses obligations de notification des violations de la sécurité des données à la ou aux autorités de contrôle compétentes ou d'information des personnes concernées par ces violations, en tenant compte de la nature du traitement des données et des informations dont il dispose.

Le donneur d'ordre prend en charge les frais engagés par le sous-traitant pour cette assistance.

8 Suspension du traitement des données

Si le sous-traitant ne respecte pas ses obligations au titre du présent contrat, le donneur d'ordre peut lui ordonner de suspendre le traitement des données jusqu'à ce qu'il se conforme au présent contrat ou que celui-ci prenne fin. Le sous-traitant informe immédiatement le donneur d'ordre s'il n'est pas en mesure, pour quelque raison que ce soit, de respecter le présent contrat.

9 Responsabilité

La responsabilité est régie par les dispositions en matière de responsabilité prévues dans les accords contractuels entre les parties.

10 Durée et résiliation

Le prestataire traite les données à caractère personnel pour une durée indéterminée jusqu'à la résiliation de la dernière convention contractuelle entre les parties concernant le traitement des données.

Le donneur d'ordre est en droit de résilier le présent contrat de manière extraordinaire et sans préavis si :

- le donneur d'ordre a suspendu le traitement des données et que le respect du présent contrat n'a pas été rétabli dans un délai raisonnable, et en tout état de cause pas dans un délai d'un mois à compter de la suspension ;
- le prestataire enfreint le présent contrat de manière significative ou persistante ou ne respecte pas les exigences applicables en matière de protection des données ;
- le sous-traitant ne se conforme pas à la décision contraignante d'une autorité de contrôle compétente ou d'un tribunal compétent portant sur les obligations du sous-traitant au regard des exigences applicables en matière de protection des données.

Le prestataire est en droit de résilier le présent contrat de manière extraordinaire et sans préavis si le donneur d'ordre insiste sur l'exécution d'un accord contractuel ou d'une instruction après avoir été informé par le prestataire que cet accord ou cette instruction enfreint les exigences applicables en matière de protection des données.

À l'expiration du présent contrat, le prestataire efface toutes les données à caractère personnel traitées pour le compte du donneur d'ordre, sauf si le prestataire est légalement ou réglementairement autorisé ou tenu de conserver ces données. Jusqu'à l'effacement des données à caractère personnel, le prestataire garantit le respect du présent contrat.

11 Dispositions finales

Le présent contrat peut être conclu sous forme électronique ou écrite. Les modifications apportées au présent contrat peuvent être effectuées sous forme électronique.

Les parties s'informent mutuellement de l'existence éventuelle d'un conseiller ou d'une conseillère en protection des données ou d'un délégué ou d'une déléguée à la protection des données, conformément aux exigences applicables en matière de protection des données.

Les parties sont tenues de traiter de manière confidentielle et durable toutes les informations relatives aux secrets d'affaires de l'autre partie ainsi qu'aux données personnelles obtenues dans le cadre du présent contrat, même après la résiliation de celui-ci, sauf si une partie est légalement tenue de procéder à une divulgation spécifique. Dans un tel cas, la partie tenue à cette obligation informe l'autre partie de cette obligation légale, pour autant que, tant que et dans la mesure où une telle information n'est pas interdite pour des raisons légales. Si une partie a des doutes quant à savoir si une information est soumise à cette obligation de confidentialité, celle-ci doit être traitée de manière confidentielle jusqu'à ce que l'autre partie en autorise expressément la divulgation.

Si certaines dispositions du présent contrat s'avéraient inapplicables, invalides ou sans effet, cela n'affecterait pas l'applicabilité, la validité ou l'efficacité des autres dispositions, et les parties remplaceraient la disposition en question par une disposition applicable, valide ou efficace qui se rapprocherait le plus possible de l'objectif visé par la disposition initiale en matière de protection des données.

Le présent contrat est exclusivement régi par le droit suisse. Le droit des conflits de lois et la Convention des Nations Unies sur les contrats de vente internationale de marchandises sont exclus. Le for juridique exclusif est le siège social du mandataire.

Annexe 1 – Catégories de données personnelles traitées

Le donneur d'ordre détermine et contrôle, à sa seule discrétion et sous sa propre responsabilité, les catégories de données personnelles qui sont traitées. Le traitement des données pour le compte du donneur d'ordre peut notamment porter sur les catégories de données personnelles suivantes :

- Données relatives à l'emploi
- Données relatives au traitement
- Métadonnées des e-mails (par exemple, expéditeur, destinataire, objet, horodatage, etc.)
- Données relatives à la vie privée
- Données relatives au statut de sécurité sociale
- Données de diagnostic
- Données relatives à la santé
- Données relatives au contenu
- Données de calendrier (par exemple, heure, lieu, titre et participants aux rendez-vous, etc.)
- Données de communication (par exemple, contenu des e-mails, historiques de chat, etc.)
- Données de contact
- Données relatives aux médicaments
- Données d'utilisation
- Données de réaction
- Données de base
- Données relatives à la description des symptômes
- Données relatives aux rendez-vous
- Données relatives aux ordonnances
- Données d'assurance
- Données relatives aux contrats
- Données de paiement
- Données d'accès aux systèmes connectés (par exemple, jetons API, données d'authentification, etc.)

Annexe 2 – Catégories de personnes concernées dont les données à caractère personnel sont traitées

Le donneur d'ordre détermine et contrôle, à sa seule discrétion et sous sa propre responsabilité, les catégories de personnes concernées dont les données à caractère personnel sont traitées. Le traitement des données pour le compte du donneur d'ordre peut notamment porter sur les catégories suivantes de données à caractère personnel :

- Interlocuteurs
- Personnes de contact
- Prestataires de services
- Contacts externes provenant de plateformes ou de services liés
- Établissements de santé
- Partenaires commerciaux
- Personnes intéressées
- Clients
- Partenaires de communication (par exemple, contacts de messagerie électronique ou d'agenda)
- Fournisseurs
- Collaborateurs
- Utilisateurs
- Patients

Annexe 3 – Mesures techniques et organisationnelles (MTO)

Les mesures techniques et organisationnelles (MTO) visant à garantir la protection et la sécurité des données personnelles traitées sont réparties comme suit : en tant que fabricant, le mandataire met à disposition l'application et est responsable de la sécurité de son logiciel et de sa base de données. L'infrastructure sous-jacente ainsi que l'environnement d'exploitation sont fournis par ServerBase AG, Suisse, en tant que prestataire de services d'hébergement.

En tant que PME suisse agile, le mandataire est spécialisé dans le développement d'applications et ne dispose délibérément pas de ses propres certifications ISO distinctes ; il garantit toutefois un niveau élevé de protection des données grâce à une méthode de travail professionnelle et à la sélection ciblée de partenaires certifiés. Il s'assure que ServerBase AG respecte toutes les mesures nécessaires conformément aux exigences applicables en matière de protection des données. Les mesures les plus importantes comprennent :

1. **Sécurité des applications et des bases de données (responsabilité du prestataire)**
    1. **Tests d'intrusion :** le framework logiciel utilisé par le prestataire est soumis à des tests d'intrusion (analyses des failles de sécurité) par des spécialistes externes.
    2. **Mise à jour continue** : l'application est entretenue en permanence par le prestataire et bénéficie des derniers correctifs de sécurité.
    3. **Surveillance proactive :** surveillance continue des performances de l'application ainsi que du serveur SQL afin de détecter immédiatement toute anomalie ou tentative d'accès non autorisée.
    4. **Séparation cryptographique et chiffrement (au repos) :** les fichiers stockés en mémoire ainsi que les champs de données sensibles au sein de la base de données sont chiffrés par défaut. Le déchiffrement est strictement limité à la clé d'organisation correspondante. Cette clé d'organisation est elle-même chiffrée cryptographiquement à l'aide de la clé utilisateur individuelle. Un accès direct au niveau des tables est techniquement impossible sans la session active de l'utilisateur et les données restent illisibles.
2. **Protection avancée en périphérie et cyberdéfense (Myra Security)**
   Myra est directement intégrée en amont de l'application en tant que bouclier de protection spécialisé à trois niveaux (proxy inverse HTTP/S). Le filtrage s'effectue conformément aux directives du RGPD de l'UE. Cela comprend :
    1. **Pare-feu d'application web hyperscale (WAF) :** filtrage continu du trafic au niveau du contenu pour combler les failles de sécurité et repousser les attaques selon le classement OWASP Top 10 (par exemple, injections SQL, cross-site scripting [XSS], traversée de répertoires).
    2. **Protection contre les attaques DDoS et les bots :** filtrage permanent et transparent des flux de trafic malveillants (attaques basées sur le volume, l'infrastructure et les applications). Grâce à l'utilisation de la plateforme Myra, le bouclier de protection est conçu pour s'adapter aux besoins et est hautement évolutif, afin de repousser efficacement même les attaques de grande envergure avant qu'elles n'atteignent l'infrastructure d'hébergement.
    3. **Équilibreur de charge multi-sites :** répartition intelligente du trafic entrant sur l'infrastructure. La détection intégrée des pannes (*Dead Backend Detection / Site Fail Over*) garantit que les serveurs temporairement

inaccessibles sont automatiquement contournés afin d'assurer une haute disponibilité (SLA d'au moins 99,9 %).

4. **Gestion automatisée des certificats :** transfert sécurisé des données grâce à l'utilisation obligatoire du protocole HTTPS, à la confidentialité parfaite (PFS) en standard, à la prise en charge du protocole HSTS, ainsi qu'à l'émission entièrement automatisée et au renouvellement en temps opportun des certificats TLS/SSL afin d'éviter toute faille de sécurité.

3. **Emplacements des centres de données et certifications (hébergement par ServerBase AG)**
    1. **Stockage des** données **en Suisse :** les données sont exclusivement stockées et traitées dans les centres de données suisses de ServerBase AG (Rümlang ZH et Lupfig AG).
    2. **Normes de conformité :** cette infrastructure est entièrement certifiée ISO 27001 et répond aux exigences de la FINMA (FINMA RS 08/7) ainsi qu'à la loi suisse sur la protection des données (LPD).
4. **Surveillance continue de la sécurité (SOC / NOC)**
    1. **Surveillance 24 h/24, 7 j/7 :** l'infrastructure réseau et serveur sous-jacente est surveillée 24 h/24, 7 j/7, 365 j/an par le Security Operations Center (SOC) dédié ainsi que par l'équipe Network Operations (NOC) de Myra, afin de détecter en temps réel les incidents de sécurité informatique et de les contrer à l'aide de niveaux d'escalade définis.
5. **Mesures de sécurité physique (ServerBase AG)**
    1. **Contrôle d'accès :** service de sécurité sur place 24 h/24, 7 j/7 pour la surveillance des centres de données et contrôles d'accès stricts à plusieurs niveaux (par exemple, scans biométriques, contrôles d'identité) afin d'empêcher tout accès non autorisé.
    2. **Protection des infrastructures :** systèmes d'extinction à gaz automatisés pour la protection contre les incendies, alimentation électrique redondante (onduleur/alimentation de secours) et systèmes de climatisation ultramodernes pour un fonctionnement optimal du matériel.
6. **Sauvegarde et restauration des données**
    1. **Sauvegardes géo-redondantes en Suisse (résidence des données garantie en Suisse) :** sauvegardes régulières et automatisées de toutes les données des clients afin d'éviter efficacement toute perte de données. Comme il s'agit de données hautement sensibles, celles-ci restent à tout moment intégralement en Suisse. Les sauvegardes cryptées sont conservées dans des locaux distincts, exclusivement dans les deux centres de données ServerBase en Suisse (Rümlang ZH et Lupfig AG).
    2. **Continuité des opérations** : processus de restauration éprouvés pour une récupération rapide des données en cas de panne (*reprise après sinistre*) ainsi qu'une maintenance proactive de l'infrastructure informatique.
7. **Assistance client sécurisée et co-navigation (Fullview)**
    1. **Cobrowsing isolé :** la technologie **Fullview** est utilisée pour l'assistance technique à la clientèle. Lors des sessions d'assistance, l'équipe d'assistance a exclusivement accès à l'onglet de navigateur isolé de l'application web. Tout accès au reste du bureau ou aux applications tierces de l'utilisateur est techniquement impossible.
    2. **Masquage automatique des données (filtre de protection des données) :** un filtre de protection des données automatique est activé pour protéger les données hautement sensibles (en particulier les données des patients). Les champs de saisie sensibles, les données personnelles ou les mots de passe

sont **automatiquement masqués** en temps réel pour le personnel d'assistance et ne sont pas transmis.

3. **Basé sur le consentement :** une session d'assistance ne peut à aucun moment être lancée à l'insu de l'utilisateur ; elle nécessite toujours l'autorisation explicite et active de l'utilisateur final.

8. **Mesures organisationnelles et justificatifs**
    1. **Sécurité interne du prestataire :** attribution pragmatique et efficace des droits (principe du « besoin d'en connaître » / principe de minimisation), utilisation systématique de l'authentification multifactorielle (MFA) pour l'accès aux systèmes, ainsi que la sensibilisation continue de ses propres collaborateurs en matière de protection des données.
    2. **Documentation :** des justificatifs relatifs à l'infrastructure (tels que les certifications ISO 27001 de ServerBase AG ou les rapports de sécurité Myra) peuvent être mis à la disposition des clients sur demande.

xatla AG Logiciels d'entreprise
Dorfmattweg 8a | 3110 Münsingen
+41 31 331 01 01 | info@xatla.ch

Annexe 4 – Liste des sous-traitants

Dans le cadre du traitement des commandes, le prestataire fait appel aux sous-traitants suivants :

- **Myra Security GmbH**, Allemagne – Mise à disposition du réseau de diffusion de contenu (CDN), de services de sécurité de pointe (pare-feu d'applications web hyperscale) et de la protection contre les attaques DDoS. Le traitement des données s'effectue en totale conformité avec les exigences de la LPD suisse et du RGPD de l'UE, exclusivement sur une infrastructure située au sein de l'Union européenne (UE).
- **cloudscale.ch AG**, Suisse – Mise à disposition d'une infrastructure numérique (hébergement cloud et services de serveurs).
- **Datadog, Inc**., États-Unis – Fourniture de services de journalisation et de surveillance (analyse et surveillance des systèmes informatiques).
- **Health Info Net AG (HIN)**, Suisse – Solutions informatiques et mise en réseau pour le secteur de la santé suisse (communication sécurisée et traitement des données).
- **Intercom Inc**., États-Unis **/ Intercom R&D Unlimited Company**, Irlande – Fourniture de services d'assistance et de communication (par ex. fonction de chat, demandes des clients, automatisation). Le traitement des données s'effectue sur la base d'un avenant de traitement des données (DPA) conclu avec des clauses contractuelles types conformément à l'art. 16, al. 2, let. d, LPD.
- **LINK Mobility Austria GmbH**, Autriche – Envoi et gestion de SMS (services de communication).
- **MediData AG**, Suisse – Solutions informatiques pour le secteur de la santé suisse (services de facturation électronique et de transmission de données).
- **Microsoft Corporation**, États-Unis / **Microsoft Ireland Operations Ltd**. – Fourniture de services cloud et de plateforme (par exemple, SignalR, composants Azure).
- **Nylas Inc**., États-Unis – Mise à disposition d'interfaces de programmation (API) pour l'accès aux données de messagerie électronique, de calendrier et de contacts dans le cadre de fonctions de communication et de gestion des rendez-vous. Le traitement des données s'effectue sur la base d'un avenant de traitement des données (DPA) conclu avec des clauses contractuelles types conformément à l'art. 16, al. 2, let. d, de la LPD.
- **Pingen AG,** Suisse – Envoi de documents de facturation sous forme numérique et physique (impression, courrier hybride). Le traitement a lieu en Suisse ; en cas de transfert vers un pays tiers, un niveau de protection des données adéquat est garanti.
- **ServerBase AG**, Suisse – Hébergement et mise à disposition d'une infrastructure numérique (gestion de serveurs et services informatiques).
- **Infomaniak Network SA**, Suisse – Mise à disposition de services d'IA conformes à la protection des données (modèles linguistiques d'IA/inférence). Le traitement et le stockage des données s'effectuent exclusivement dans les centres de données propres à Infomaniak en Suisse, certifiés ISO 27001 et ISO 50001. Tout transfert de données vers des pays tiers ou des prestataires tiers à des fins d'entraînement est techniquement et contractuellement exclu.
- **Fullview ApS, Danemark** – Fourniture d'outils d'assistance visuelle (cobrowsing et infrastructure d'assistance client). Le traitement des données s'effectue conformément au RGPD et à la DSG exclusivement sur des serveurs situés au sein de l'Union européenne (région de Francfort, Allemagne). Les champs de données sensibles sont masqués par le système avant leur transmission (masquage des données).