SeniorContact

Mesures techniques et organisationnelles (TOM)

Dernière mise à jour: 04.08.2026

1. Historique

04.08.2026 — Première version publique

2. À propos de ce document

Ce document décrit les principales mesures techniques et organisationnelles (TOM) mises en place par SeniorContact Sàrl (IDE : CHE-304.129.551) pour protéger les données personnelles traitées dans le cadre du site web, de l'application mobile, de l'API / backend et des outils d'administration SeniorContact.

Il vise à répondre aux exigences des articles 7 et 8 de la Loi fédérale sur la protection des données (LPD / nLPD), de l'article 3 de l'Ordonnance sur la protection des données (OPDo), et, à titre de bonne pratique, de l'article 32 du RGPD.

Périmètre : mesures appliquées par SeniorContact en tant que responsable du traitement pour le Service. L'hébergement et l'infrastructure associée en Suisse sont fournis par Infomaniak ; la sécurité physique des centres de données et les contrôles de la plateforme d'hébergement sont décrits dans les TOM et le DPA d'Infomaniak. Les autres sous-traitants appliquent leurs propres mesures dans le cadre de leurs contrats avec nous (voir notre liste publique de sous-traitants).

Les mesures sont choisies de manière proportionnée au risque et à la nature des traitements (y compris le contexte d'usage par des aidants et des seniors). Aucun système n'est sans risque ; nous améliorons nos protections dans le temps.

3. Confidentialité

3.1. Sécurité physique

- Les serveurs d'application, bases de données et stockages objets de production utilisés pour le Service sont hébergés en Suisse par Infomaniak (région de Genève).
- L'accès physique aux centres de données est contrôlé par Infomaniak selon son programme de sécurité et ses TOM.
- SeniorContact n'exploite pas son propre centre de données. Les postes utilisés pour l'administration sont limités aux personnes autorisées.

3.2. Contrôle des accès aux systèmes et aux données

- L'accès aux systèmes de production, à la console d'administration et aux consoles des prestataires est limité à un nombre restreint de personnes autorisées.
- Les services d'administration et d'exploitation sensibles ne sont pas exposés librement sur l'internet public : l'accès réseau est restreint (réseau privé / accès contrôlé), puis protégé par authentification.
- Les secrets d'exploitation sont gérés de manière sécurisée, en dehors du code source de l'application.
- Les comptes utilisateurs sont authentifiés (e-mail / mot de passe et/ou connexion sociale le cas échéant). Les mots de passe stockés par SeniorContact sont hachés ; ils ne sont pas conservés en clair. Une longueur minimale de mot de passe est exigée.
- Les tentatives d'authentification sont limitées afin de réduire les attaques automatisées.
- L'accès administratif au Service est distinct des comptes utilisateurs finaux.
- Les sessions et jetons d'authentification sont soumis à des mécanismes d'expiration et peuvent être invalidés lorsque cela est nécessaire, notamment pour des raisons de sécurité.
- Les accès administratifs aux systèmes de production et aux consoles des prestataires critiques sont protégés par une authentification multifacteur (MFA), lorsque cette fonctionnalité est disponible.
- Les droits d'accès sont attribués selon le principe du moindre privilège et limités aux besoins opérationnels. Ils sont retirés ou adaptés lorsqu'une personne n'en a plus besoin, notamment en cas de changement de rôle ou de départ.
- Les comptes administratifs sont individuels dans la mesure où les systèmes concernés le permettent ; le partage de comptes administratifs est évité.

- Les comptes chez les sous-traitants sont limités aux comptes opérationnels nécessaires au Service.

3.3. Chiffrement et sécurité des transferts

- Les communications avec le site, l'API et les applications utilisent des connexions chiffrées (HTTPS / TLS) en production.
- Certains champs sensibles (notamment certains contenus de messages et éléments liés aux médias) sont chiffrés au niveau applicatif avant stockage, lorsque cela est mis en œuvre dans notre backend. Les secrets et clés nécessaires aux mécanismes cryptographiques sont gérés séparément du code source et leur accès est limité aux composants et personnes qui en ont besoin.
- Les postes de travail utilisés pour administrer le Service sont protégés par le chiffrement du disque, afin de limiter l'impact en cas de vol ou de perte.
- Le traitement vidéo peut passer par un prestataire temporaire ; les vidéos sont ensuite migrées vers le stockage Infomaniak puis retirées du prestataire temporaire selon notre pratique de conservation.

3.4. Séparation et moindre privilège

- Les environnements de production sont séparés des environnements de développement et de test. L'accès à la production est limité aux personnes et systèmes autorisés.
- Les utilisateurs finaux n'accèdent qu'aux données de leur compte / relations autorisées (ex. lien aidant–senior).
- L'accès admin aux données personnelles est limité à l'exploitation et au support du Service.
- Les données personnelles issues de la production ne sont pas utilisées dans les environnements de développement ou de test, sauf nécessité particulière assortie de mesures de protection appropriées.

3.5. Personnel et confidentialité

- Les personnes ayant accès aux systèmes ou aux données personnelles sont tenues à la confidentialité.
- Lorsque de nouvelles personnes obtiennent un accès, une sensibilisation proportionnée à la sécurité et à la protection des données leur est fournie.

3.6. Fin de vie des supports et documents

- Les documents papier sensibles, s'il y en a, sont détruits de manière à rendre la récupération des informations impraticable (ex. broyage).
- Les supports numériques mis hors service (disques, postes) sont effacés ou détruits de manière appropriée avant réemploi ou élimination.

4. Intégrité

4.1. Gestion des changements et des versions

- Le code applicatif est versionné.
- Les déploiements en production sont effectués par des personnes autorisées ; l'accès à la production est restreint (voir § 3.2).
- Les dépendances et plateformes sont mises à jour lorsque des correctifs de sécurité sont pertinents et praticables.
- Les vulnérabilités affectant les composants utilisés par le Service sont évaluées en fonction de leur gravité, de leur exploitabilité et de leur exposition.
- Les vulnérabilités présentant un risque important font l'objet d'une correction ou de mesures compensatoires prioritaires.
- Les dépendances applicatives font l'objet d'un suivi afin d'identifier les mises à jour et vulnérabilités de sécurité pertinentes.

4.2. Journalisation et surveillance

- Des journaux techniques sont collectés pour exploiter, protéger et dépanner le Service.
- Les journaux sont conservés pendant une durée limitée, comme indiqué dans notre Politique de confidentialité.
- Un comportement anormal peut être investigué à l'aide de ces journaux et des alertes des prestataires.

• L’accès aux journaux est limité aux personnes et systèmes qui en ont besoin à des fins d’exploitation, de sécurité ou d’investigation.

• Lorsque cela est techniquement disponible, des alertes sont utilisées afin d’identifier certains événements susceptibles d’indiquer un incident, un abus ou un comportement anormal.

• Les journaux sont conçus pour limiter l’enregistrement inutile de données personnelles et de secrets techniques.

4.3. Contrôle des transferts

• Les données en transit vers et depuis le Service sont protégées par TLS lorsque le Service est accessible via l’internet public.

• Les transferts vers les sous-traitants sont limités à ce qui est nécessaire pour fournir le Service et encadrés par des contrats / DPA et notre Politique de confidentialité, lorsque applicable.

• Une liste publique des principaux sous-traitants est publiée sur notre site.

4.4. Organisation de la protection des données

• SeniorContact Sàrl est responsable de la conformité en matière de protection des données pour le Service.

• Les informations de confidentialité sont publiées (Politique de confidentialité, cookies, liste des sous-traitants, le présent document TOM).

• Les demandes des personnes concernées (accès, rectification, suppression, etc.) peuvent être adressées à support@seniorcontact.app ; une vérification d’identité peut être exigée.

• La suppression de compte est proposée via le Service / un parcours dédié, sous réserve des obligations légales de conservation.

• Nous ne stockons pas les données de carte de paiement ; les paiements in-app sont traités par les plateformes et prestataires de paiement concernés (voir la liste des sous-traitants).

4.5. Tests de sécurité

• La sécurité du Service s’appuie sur des revues internes dans le cadre du développement, sur la mise à jour des composants, et sur les mesures de l’hébergeur. SeniorContact n’a pas, à ce stade, mandaté de test d’intrusion externe. Des tests de sécurité complémentaires, y compris des tests d’intrusion, peuvent être réalisés lorsque le risque ou l’évolution du Service le justifie.

5. Disponibilité et fiabilité

5.1. Hébergement, sauvegardes et restauration

• L’hébergement, le stockage et les sauvegardes de l’infrastructure centrale s’appuient sur les plateformes Infomaniak en Suisse.

• Un stockage objet est utilisé pour les médias utilisateurs (images, audio et vidéos, le cas échéant après traitement temporaire).

• En cas d’incident affectant la disponibilité, la restauration des données s’appuie sur les mécanismes de sauvegarde du prestataire d’hébergement.

• Les mécanismes de sauvegarde et de restauration font l’objet de vérifications périodiques afin de s’assurer qu’une restauration des données peut être réalisée en cas de besoin.

• L’accès aux sauvegardes est limité aux personnes et systèmes autorisés.

• La stratégie de sauvegarde et de restauration tient compte de la criticité des données et services concernés.

5.2. Protection réseau et edge

• Des protections réseau et edge sont utilisées pour certaines fonctions du Service (y compris liées aux appels), en complément des protections du prestataire d’hébergement.

• L’accès aux services d’administration est restreint au niveau réseau, ce qui réduit la surface d’attaque exposée sur l’internet public.

5.3. Gestion des incidents

- SeniorContact dispose d’un processus de gestion des incidents de sécurité permettant d’identifier, qualifier, contenir, investiguer et traiter les incidents affectant la confidentialité, l’intégrité ou la disponibilité des données et systèmes.
- Les éléments utiles à l’investigation sont préservés lorsque cela est nécessaire et proportionné.
- Après un incident significatif, les causes et mesures correctives peuvent faire l’objet d’une analyse afin de réduire le risque de récurrence.
- Les violations de la sécurité des données personnelles sont évaluées afin de déterminer les obligations de notification applicables. Les autorités compétentes et/ou les personnes concernées sont informées lorsque le droit applicable l’exige.
- Contact pour les questions de confidentialité et de sécurité : support@seniorcontact.app.

5.4. Maintenance des systèmes

- Les systèmes d’exploitation, composants, services managés et dépendances applicatives font l’objet de mises à jour de sécurité en fonction des risques identifiés et des correctifs disponibles.
- Le chat d’assistance est auto-hébergé sur notre infrastructure Infomaniak, dans le même périmètre d’hébergement.

6. Traçabilité

- Les journaux d’authentification et d’exploitation permettent d’investiguer les accès et incidents.
- Les opérations administratives pertinentes pour la sécurité et la protection des données sont associées, dans les journaux disponibles, au compte administratif authentifié ayant réalisé l’action.
- L’accès aux journaux est restreint et leur conservation est limitée aux durées nécessaires aux finalités de sécurité, d’exploitation, d’investigation et de prévention des abus.
- La conservation des journaux est limitée et liée à des finalités (sécurité, fiabilité, prévention des abus).

7. Mesures des sous-traitants

Lorsque Infomaniak ou un autre sous-traitant traite des données personnelles pour notre compte, leurs TOM / documentations de sécurité contractuelles complètent le présent document pour la partie du traitement qu’ils réalisent. Des accords de traitement (DPA) sont en place pour les principaux sous-traitants techniques ; les accords avec certains prestataires (ex. fiduciaire / comptable) peuvent être formalisés séparément.