SeniorContact

Technical and organisational measures (TOMs)

Last updated: 2026-08-04

1. Document history

2026-08-04 — First public version

2. About this document

This document describes the main technical and organisational measures (TOMs) implemented by SeniorContact Sàrl (IDE: CHE-304.129.551) to protect personal data processed in connection with the SeniorContact website, mobile application, API/backend and administration tools.

It is intended to meet the requirements of Articles 7 and 8 of the Swiss Federal Act on Data Protection (FADP / nLPD), Article 3 of the Data Protection Ordinance (DPO / OPDo), and, as a matter of good practice, Article 32 GDPR.

Scope: measures applied by SeniorContact as controller for the Service. Hosting and related infrastructure in Switzerland are provided by Infomaniak; physical security of data centres and hosting-platform controls are described in Infomaniak's own TOMs and DPA. Other sub-processors apply their own measures under their contracts with us (see our public sub-processors list).

Measures are chosen in proportion to the risk and to the nature of the processing (including use by caregivers and seniors). No system is risk-free; we improve our safeguards over time.

3. Confidentiality

3.1. Physical security

- Production application servers, databases and object storage used for the Service are hosted in Switzerland by Infomaniak (Geneva area).
- Physical access to data centres is controlled by Infomaniak according to its security programme and TOMs.
- SeniorContact does not operate its own data centre. Workstations used for administration are limited to authorised persons.

3.2. Access control to systems and data

- Access to production systems, the admin console and provider consoles is limited to a small number of authorised persons.
- Sensitive administration and operations services are not freely exposed on the public internet: network access is restricted (private / controlled access), then protected by authentication.
- Operational secrets are managed securely, outside the application source code.
- User accounts are authenticated (email/password and/or social sign-in providers where enabled). Passwords stored by SeniorContact are hashed and are not kept in clear text. A minimum password length is required.
- Authentication attempts are limited to reduce automated attacks.
- Administrative access to the Service is separate from end-user accounts.
- Authentication sessions and tokens are subject to expiry mechanisms and may be invalidated when necessary, including for security reasons.
- Administrative access to production systems and critical provider consoles is protected by multi-factor authentication (MFA), where this feature is available.
- Access rights are granted according to the principle of least privilege and limited to operational needs. They are withdrawn or adjusted when a person no longer needs them, including in the event of a change of role or departure.
- Administrative accounts are individual insofar as the systems concerned allow it; sharing of administrative accounts is avoided.
- Sub-processor accounts are limited to operational accounts used to run the Service.

3.3. Encryption and transport security

- Communications with the website, API and apps use encrypted connections (HTTPS / TLS) in production.
- Sensitive fields (including certain message and media-related content) are encrypted at application level before storage where implemented in our backend. Secrets and keys required for cryptographic mechanisms are managed separately from the source code and access to them is limited to the components and persons that need them.
- Workstations used to administer the Service are protected with full-disk encryption, to limit impact if a device is lost or stolen.
- Video processing may use a temporary provider; videos are then migrated to Infomaniak storage and removed from the temporary provider according to our retention practice.

3.4. Separation and least privilege

- Production environments are separated from development and test environments. Access to production is limited to authorised persons and systems.
- End users only access data belonging to their account / authorised relationships (e.g. caregiver–senior links).
- Admin access to personal data is limited to operating and supporting the Service.
- Personal data from production is not used in development or test environments, except where specifically necessary and subject to appropriate protective measures.

3.5. Personnel and confidentiality

- People with access to systems or personal data are bound by confidentiality.
- When additional people are given access, proportionate security and data-protection awareness is provided.

3.6. End-of-life of media and documents

- Sensitive paper documents, if any, are destroyed so that information recovery is impractical (e.g. shredding).
- Decommissioned digital media (disks, workstations) are wiped or destroyed appropriately before reuse or disposal.

4. Integrity

4.1. Change and release management

- Application code is version-controlled.
- Production deployments are performed by authorised persons; production access is restricted (see § 3.2).
- Dependencies and platforms are updated when security fixes are relevant and practicable.
- Vulnerabilities affecting components used by the Service are assessed according to their severity, exploitability and exposure.
- Vulnerabilities presenting a significant risk are subject to priority remediation or compensating measures.
- Application dependencies are monitored in order to identify relevant security updates and vulnerabilities.

4.2. Logging and monitoring

- Technical logs are collected to operate, protect and troubleshoot the Service.
- Logs are retained for a limited period as described in our Privacy Policy.
- Abnormal behaviour may be investigated using these logs and provider alerts.
- Access to logs is limited to the persons and systems that need them for operations, security or investigation purposes.
- Where technically available, alerts are used to identify certain events that may indicate an incident, abuse or abnormal behaviour.
- Logs are designed to limit unnecessary recording of personal data and technical secrets.

4.3. Transfer control

- Data in transit to and from the Service is protected with TLS where the Service is accessed over the public internet.
- Transfers to sub-processors are limited to what is needed to provide the Service and are governed by contracts / DPAs and our Privacy Policy where applicable.

- A public list of main sub-processors is published on our website.

4.4. Data protection organisation

- SeniorContact Sàrl is responsible for data protection compliance for the Service.
- Privacy information is published (Privacy Policy, cookie policy, sub-processors list, this TOMs document).
- Data subject requests (access, correction, deletion, etc.) can be sent to support@seniorcontact.app; identity may be verified before processing.
- Account deletion is offered via the Service / dedicated deletion flow, subject to legal retention duties.
- We do not store payment card data; in-app payments are handled by the relevant payment platforms and providers (see the sub-processors list).

4.5. Security testing

- The security of the Service relies on internal reviews as part of development, on component updates, and on the hosting provider's measures. SeniorContact has not, at this stage, commissioned an external penetration test. Complementary security tests, including penetration tests, may be carried out when the risk or the evolution of the Service justifies it.

5. Availability and reliability

5.1. Hosting, backups and restore

- Hosting, storage and backups for core infrastructure rely on Infomaniak platforms in Switzerland.
- Object storage is used for user media (images, audio and videos, where applicable after temporary processing).
- If an incident affects availability, data restore relies on the hosting provider's backup mechanisms.
- Backup and restore mechanisms are subject to periodic checks to ensure that data can be restored if needed.
- Access to backups is limited to authorised persons and systems.
- The backup and restore strategy takes into account the criticality of the data and services concerned.

5.2. Network and edge protection

- Network and edge protections are used for certain Service features (including call-related functions), in addition to the hosting provider's protections.
- Access to administration services is restricted at the network level, which reduces the attack surface exposed on the public internet.

5.3. Incident handling

- SeniorContact has a security incident management process enabling it to identify, qualify, contain, investigate and address incidents affecting the confidentiality, integrity or availability of data and systems.
- Elements useful for investigation are preserved when necessary and proportionate.
- After a significant incident, causes and corrective measures may be analysed in order to reduce the risk of recurrence.
- Personal data security breaches are assessed in order to determine applicable notification obligations. Competent authorities and/or data subjects are informed when required by applicable law.
- Contact for privacy and security matters: support@seniorcontact.app.

5.4. System maintenance

- Operating systems, components, managed services and application dependencies are subject to security updates according to identified risks and available patches.
- Support chat is self-hosted on our Infomaniak infrastructure, under the same hosting perimeter.

6. Traceability

- Authentication and operational logs support investigation of access and incidents.
- Administrative operations relevant to security and data protection are associated, in the available logs, with the authenticated administrative account that performed the action.

- Access to logs is restricted and their retention is limited to the periods necessary for the purposes of security, operations, investigation and abuse prevention.
- Retention of logs is limited and purpose-bound (security, reliability, abuse prevention).

7. Sub-processors' measures

Where Infomaniak or another sub-processor processes personal data on our behalf, their contractual TOMs / security documentation complement this document for the parts of the processing they perform. Data processing agreements (DPAs) are in place for the main technical sub-processors; agreements with certain providers (e.g. fiduciary / accountant) may be formalised separately.