JIFELINE NETWORKS

Technical and Organizational Measures

Appendix to our Data Processing Agreement (GDPR)

Version 1.1 (2026)

Document history

This policy falls under documented information in accordance with ISO 27001. Version control is maintained in the document history. Only authorized persons may make changes. Retention periods and access rights are defined in the ISMS.

Revisions

Version	Date	Author	Review
Version 1.0	14-3-2024	Wouter van Hiele	Management, ICT, Legal, Security & Compliance Team
Version 1.1	5-1-2026	Wouter van Hiele	Management, ICT, Legal, Security & Compliance Team

Approval

Name	Role	Version	Date
Geert van der Hoek	CEO	1.1	30-1-2026

Document classification

Classification	Description
Public	This document may be shared outside the organization without risk. No confidentiality restrictions apply.

Technical and Organizational Measures (TOM)

According to Art. 32 GDPR

1. General Considerations

This document describes the technical and organizational measures implemented by Jifeline Networks B.V. to meet legal and contractual requirements when processing personal data. It takes into account the rights of data subjects and requirements of the articles 24, 25, and 32 GDPR to the extent applicable.

The measures described in this document serve the purpose:

- to encrypt or pseudonymize personal data where necessary,
- to ensure the confidentiality, integrity, availability and resilience of systems and services in connection with the processing of personal data,
- to restore the availability of and access to personal data in the event of a physical or technical incident in a timely manner, and
- to regularly review, assess and evaluate the effectiveness of all technical and organizational measures to ensure the security of processing.

The following measures apply to all data processing activities that are under control of Jifeline Networks B.V., or where Jifeline Networks B.V. is a subcontracted data processor on behalf of another data controller. In situations where Jifeline Networks B.V. is the data controller and another organization is the data processor on behalf of Jifeline Networks B.V., Jifeline Networks B.V. aims at ensuring that the technical and organizational measures implemented by the subcontracted processor equals at minimum the processing security level indicated by following measures.

Please note: In federated service delivery scenarios, one or more data controllers and one or more subcontracted data processors may be entrusted with or involved in processing personal data.

2. Physical Security

2.1 Corporate facility security

Physical secure areas (zones) are defined on the basis of information security and data protection requirements and protected against unauthorized access by appropriate physical safeguards. The physical security concept distinguishes between public areas (parking, reception), controlled areas, restricted/internal areas, and high-risk zones. Secure zones are defined based on the protection needs of the information assets housed or made accessible within them. (such as server rooms, HR department).
Depending on the specific zone classification, selected or all of the following security features are implemented: Access restriction through personalized access medium, video surveillance. For dealing with visitors and deliveries, procedures are used to prevent unauthorized persons from accessing security areas.

2.2 SaaS Services Data Center Security

Jifeline Networks B.V. uses Amazon Web Services (AWS) data centers for hosting its services. Jifeline Networks B.V. shall regularly review AWS compliance documentation to ensure continued alignment with GDPR requirements.

2.3 Access Control

All access rights (both for access to IT systems and data and for access to buildings and rooms) are assigned according to the principle that employees and third-party users are only granted the level of access they need to perform their activities (need-to-know principle).

Access rights are granted according to defined (role-based) permission profiles. The access rights granted are reviewed monthly or yearly depending on the system. Rights that are no longer required are withdrawn immediately. Access to networks and network services is restricted by technical and physical measures.

To prevent unauthorized people from entering our building, but also to prevent unauthorized (electronic) access to IT systems, Jifeline Networks B.V. has implemented measures including, but not limited to:

- For every employee, a personally assigned user is set up with a password bound to strict requirements (at least 10 characters long with special characters).
- Passwords must be unique and may not be used for other accounts.
- A password manager is used for storing credentials.
- User-dependent authentication; through Single-Sign-On with company Identity Provider where possible, or at minimum username and password combined with 2FA.
- For certain high risk resources IP whitelisting is used or VPN is required.
- Access is monitored and logged 24x7, including unsuccessful login attempts.
- Only employees get access to the majority of files and systems and the extent of access can be determined selectively based on need to know principle.

3. Operational Security

3.1 Transfer Control

Mechanisms for securing data traffic and communication connections, as well as for monitoring and logging activities in networks, have been established to the required extent. As appropriate, firewalls and intrusion detection and prevention systems (IDS / IPS) are in place.

When personal data is transmitted via public communication networks, secure end-to-end encryption of the communication is ensured. Secure connections (VPN tunnels) are used for access to IT resources via public networks.
If the exchange of confidential authentication information is required, this is done via a different communication path than the actual data transmission. When transporting personal data stored on data carriers, the use of encryption or a passcode ensures that the data is protected against unauthorized access, manipulation or loss. After transport, the data is deleted from the storage media used for transport if it is no longer required on them.

Paper printouts and exports of confidential data from their source system are avoided whenever possible or otherwise printed by a secure printing solution. Hard copies and electronic exports of confidential information leaving the business premises are handled with special care, taking into account the relevant confidentiality level - with the aim of preventing disclosure, loss and unauthorized copying. As soon as a paper printout is no longer required, it is destroyed. Electronic data exports that are no longer required are deleted again from the respective storage location and any transport data carrier used.

3.2 Input Control

Measures for subsequent verification of whether and by whom data has been entered, changed or removed (deleted) are implemented to the extent necessary. In systems used to collect and process personal data, access is categorized and automatically recorded. Assigning, Changing and deleting user authorizations are logged. The integrity of log information is ensured.

3.3 Availability and Reliability

In leveraging AWS as cloud provider, Jifeline Networks B.V. ensures the availability and reliability of infrastructure and processed data through strategic deployment across multiple geographically dispersed data centers, adherence to AWS Service Level Agreements, implementation of robust redundancy, disaster recovery planning, continuous monitoring, and compliance with industry-leading security measures. Processes or procedures for handling disruptions to internal IT systems and for restoring systems after a disruption have been established to the extent required.

3.4 Usage Control

Jifeline Networks B.V. has implemented the following measures when working within software systems:

- The password rules for access control must also be followed for usage control.
- Role-based authorization, administrative user profiles are kept to a minimum.
- User-dependent authentication through Single-Sign-On with company Identity Provider where possible, or at minimum username and password combined with 2FA.
- The use of personal data is limited, so that only authorized individuals can use the personal data necessary for their task.
- Audit logging of usage and changes.

- Paperless work by principle and compliant destruction of paper documents with a shredder.

3.5 Network Security

Jifeline Networks B.V. has implemented industry standard technologies and controls to protect network security, including firewalls, VPN, segregation, IP whitelisting and wireless security. Networks are designed and configured to restrict connections between trusted and untrusted networks, and network designs and controls shall be reviewed at least annually to ensure they remain effective and up to date.

4. Product Development

In software and hardware development, Jifeline Networks B.V. adheres to 'privacy by default' and 'secure by default' principles, integrating strong safeguards to ensure robust data protection and system security.

4.1 Development Tools

- Where possible, single-sign-on authentication is used for third party applications to allow for a complete and compliant access administration within the organization.
- Development tools are only downloaded from secure sources (e.g., the manufacturer's servers).

4.2 Secure Development

Jifeline Networks B.V. has implemented a secure software development lifecycle (SDLC) that includes security testing, code reviews and dependency checks before implementing software in production environment. Test-, Accept- and Production- environments are completely separated environments.

4.3 Privacy-Friendly Settings

- Product development takes into account giving users the option of entering only the information necessary for the purpose of processing. Input fields with additional, unnecessary information are avoided or at least designed as non-mandatory.
- By default, privacy-friendly settings are preselected.
- By default, explicit user consent is requested for data processing.

4.4 Pseudonymization

Personal Identifiable Information (PII) is pseudonymized so far as the connection to the individual is not absolutely necessary for the result.

4.5 Data Deletion

Jifeline Networks B.V. ensures that personal data is retained only for the necessary duration and explicitly defines data retention periods.

4.6 Change Management

Jifeline Networks B.V. maintains change management policies and procedures to plan, test, schedule, communicate, and execute changes to its infrastructure, systems, networks, and applications.

5. Employee Security

Jifeline Networks B.V. has implemented measures for their employees developing or accessing customer data and systems including, but not limited to:

- Employees must encrypt their hard drives with state-of-the-art encryption, e.g. BitLocker, Apple FileVault or equivalent software for other operating systems.
- The online work environment provider applies a default virus, spam and phishing filter to detect malicious software and avert cyber-attacks.
- EDR software is utilized to all its employees to detect and remediate malware, viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorized access to information or systems.
- Office wireless and wired networks are segregated, redundant and protected by Firewalls.
- Employees are obligated to clean their desk of any documents containing sensitive data, especially when accessible by others.
- Employees are obligated to lock their devices when leaving their workplace.

5.1 Background Screening

Employees with access to customer personal data shall undergo background screening, compliant with local (data protection) laws and regulations, limited to what is necessary for their role.

5.2 Confidentiality Obligations

Employees with access to customer personal data shall be subject to binding contractual obligations with Jifeline Networks B.V. to maintain confidentiality.

5.3 Security Awareness Training

Employees receive training upon hire and at least annually, covering security best practices and privacy principles. Training completion is tracked and documented.

6. Procedure for Regular Review, Assessment and Evaluation

Information on potential technical vulnerabilities or errors in data processing systems (IT systems) is evaluated at regular intervals and appropriate measures are initiated. Critical patches are deployed as soon as possible for both operating systems and software applications in use. Data processing systems (IT systems) are checked regularly to the extent required and after changes to ensure that they are functioning properly.

Jifeline Networks B.V. has implemented the following internal measures:

- Appointment of a Security Officer
- Regular testing of employee Security Awareness
- Regular auditing of procedures
- Regular review of technical advancements in accordance with Article 32 GDPR