Verifeye Online
Trust Services Practice Statement

Title: Verifeye Online Trust Services Practice Statement

Date: 14.01.2026

Name: Christopher Gray

Classification: Public

Version: V 2.0

Contents

1 Introduction 5
1.1 Overview 5
1.2 Document Name and Identification 5
1.3 PKI Participants 6
1.3.1 Certification Authorities 6
1.3.2 Registration Authorities 6
1.3.3 Subscribers 6
1.3.4 Relying Parties 6
1.3.5 Subcontractors 6
1.4 Certificate Usage 6
1.5 Policy Administration 7
1.5.1 Organization Administering the Document 7
1.5.2 Contact Person 7
1.5.3 Person Determining CPS Suitability for the Policy 7
1.5.4 TSPS Approval Procedures 7
1.6 Definitions and Acronyms 7
1.6.1 Definitions 7
1.6.2 Acronyms 7
1.6.3 References 7
2 Publication and Repository Responsibilities 8
2.1 Repositories 8
2.2 Publication of Certificate Information 8
2.3 Time or Frequency of Publication 8
2.4 Access Controls on Repositories 8
3 Identification and Authentication 8
3.1 Naming 8
3.2 Initial Identity Validation 9
3.2.1 Method to Prove Possession of Private Key 9
3.2.2 Authentication of Organization Entity 9
3.2.3 Authentication of Individual Identity 9
3.2.4 Non-verified Subscriber Information 9
3.2.5 Validation of Authority 9
3.2.6 Criteria for Interoperation 10
3.3 Identification and Authentication for Re-key Requests 10
3.4 Identification and Authentication for Revocation Requests 10
4. Certificate Life-Cycle Operational Requirements 10
5. Facility, Management, and Operational Controls 10
5.1 Physical Controls 10
5.1.1 Site Location and Construction 10

5.1.2 Physical Access 11
5.1.3 Power and Air Conditioning 11
5.1.4 Water Exposure 11
5.1.5 Fire Prevention and Protection 11
5.1.6 Media Storage 11
5.1.7 Waste Disposal 12
5.1.8 Off-site backup 12
5.2 Procedural Controls 12
5.2.1 Trusted Roles 12
5.2.2 Number of Persons Required per Task 13
5.2.3 Identification and Authentication for Each Role 13
5.2.4 Roles Requiring Separation of Duties 13
5.3 Personnel Controls 13
5.3.1 Qualification, Experience, and Clearance Requirements 14
5.3.2 Background Check Procedures 14
5.3.3 Training Requirements 14
5.3.4 Re-Training Frequency and Requirements 14
5.3.5 Job Rotation Frequency and Sequence 15
5.3.6 Sanctions for Unauthorized Actions 15
5.3.7 Independent Contractor Requirements 15
5.3.8 Documentation Supplied to Personnel 15
5.4 Audit Logging Procedures 15
5.4.1 Types of Events Logged 15
5.4.2 Frequency of Processing Log 15
5.4.3 Retention Period for Audit Log 16
5.4.4 Protection of Audit Log 16
5.4.5 Audit Log Backup Procedures 16
5.4.6 Audit Collection System (Internal vs. External) 16
5.4.7 Notification to Event-Causing Subject 16
5.5 Records Archival 16
5.5.1 Types of Records Archived 16
5.5.2 Retention Period for Archive 16
5.5.3 Protection of Archive 17
5.5.4 Archive Backup Procedures 17
5.5.5 Requirements for Time Stamping of Records 17
5.5.6 Archive Collection System (Internal or External) 17
5.5.7 Procedures to Obtain and Verify Archive Information 17
5.6 Key Changeover 17
5.7 Compromise and Disaster Recovery 17
5.7.1 Incident and Compromise Handling Procedures 17
5.7.2 Computing Resources, Software, and/or Data are Corrupted 18
5.7.3 Entity Private Key Compromise Procedures 18
5.7.4 Business Continuity Capabilities after a Disaster 18
5.8 CA or RA Termination 19
5.8.1 Termination of Identification Service 19

6 Technical Security Controls....19
6.1 Key Pair Generation and Installation.... 19
6.2 Private Key Protection and Cryptographic Module Engineering Controls....19
6.3 Other Aspects of Key Pair Management....20
6.4 Activation Data....20
6.5 Computer Security Controls....20
6.5.1 Specific Computer Security Technical Requirements.... 20
6.5.2 Computer Security Rating....21
6.6 Life Cycle Technical Controls....21
6.6.1 System Development Controls....21
6.6.2 Security Management Controls....21
6.6.3 Life Cycle Security Controls....21
6.6.4 Network security controls....21
6.7 Time stamping....22
7 Certificate, CRL, and OCSP Profiles....22
8 Compliance Audit and Other Assessments....23
8.1 Frequency and Circumstances of Assessment....23
8.2 Identity/Qualifications of Assessor.... 23
8.3 Assessor's Relationship to Assessed Entity.... 23
8.4 Topics Covered by Assessment....23
8.5 Actions Taken as a Result of Deficiency.... 23
8.6 Communications of Results.... 24
9 Other Business and Legal Matters....24
9.1 Fees.... 24
9.2 Financial Responsibility....24
9.2.1 Insurance Coverage....24
9.2.2 Other Assets.... 24
9.3 Confidentiality of Business Information....24
9.3.1 Scope of Confidential Information....24
9.3.2 Information Not Within the Scope of Confidential Information.... 24
9.3.3 Responsibility to Protect Confidential Information.... 24
9.4 Privacy of personal information....24
9.4.1 Privacy Plan.... 25
9.4.2 Information Treated as Private....25
9.4.3 Information not Deemed Private.... 25
9.4.4 Responsibility to Protect Private Information.... 25
9.4.5 Notice and Consent to Use Private Information....25
9.4.6 Disclosure Pursuant to Judicial or Administrative Process.... 25
9.4.7 Other Information Disclosure Circumstances....25
9.5 Intellectual Property Rights.... 25
9.6 Representations and Warranties....25
9.6.1 CA Representations and Warranties....25
9.6.2 RA Representations and Warranties....25
9.6.3 Subscriber Representations and Warranties.... 26
9.6.4 Relying Party Representations and Warranties.... 26

9.6.5 Representations and warranties of other participants....26
9.7 Disclaimers of Warranties....26
9.8 Limitations of Liability....26
9.9 Indemnities....26
9.9.1 Indemnification by Subscribers....26
9.10 Term and Termination....27
9.10.1 Term....27
9.10.2 Termination....27
9.10.3 Effect of Termination and Survival....27
9.11 Individual notices and communications with participants....27
9.12 Amendments....27
9.12.1 Procedure for Amendment....27
9.12.2 Notification Mechanism and Period....27
9.12.3 Circumstances under Which OID Must be Changed....27
9.13 Dispute Resolution Provisions....27
9.14 Governing Law....27
9.15 Compliance with Applicable Law....28
9.16 Miscellaneous provisions....28
9.16.1 Entire agreement....28
9.16.2 Assignment....28
9.16.3 Severability....28
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)....28
9.16.5 Force Majeure....28
9.17 Other provisions: Obligation of Service Provider....28
10 Document Maintenance....30
11 Document History....30

1 Introduction

Verifeye Online, Sia is an identity service provider offering online services for identity verification of natural persons (in the following “persons” or “users”) in order to support Verifeye’s partners needing reliable identification of their users.

In addition, in collaboration with qualified trust service providers and contract partners Verifeye enables individual users of the contracted partners (in the following “partners”) to electronically sign legally binding contracts using qualified electronic signatures according to the eIDAS regulation.

The identity verification services are compliant with the requirements of the German Anti-Money Laundering Regulation and the Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

In particular, Verifeye verifies the identity of natural persons amongst other methods in accordance with the new eIDAS regulation, Article 24, paragraph 1a c) by using “other identification methods” recognized in Germany which ensure the identification of the person with a high level of confidence.

The technical specifications and procedures implemented by Verifeye fulfil the requirements of article 20 and 21 of eIDAS and the requirements of the applicable parts of ETSI EN 319 401 and ETSI EN 319 411-1/2. Verifeye Online’s services are also in conformance with the German Geldwäschegesetz (prevention of money laundering act)

This document is the Trust Service Practice Statement (TSPS) of Verifeye Online, Sia. It is not a full Certification Practice Statement (CPS) according to RFC 3647 because Verifeye only provides identity verification services, but does currently not offer other certification services like issuing certificates or the provision of certificate validation services.

The purpose of this document is to serve as a base for compliance with eIDAS.

1.1 Overview

Verieye Online’s services allow customers of contract partners to be reliably identified using online video conferencing for identification while the customer is at home or at his/her workplace. Verifeye Online delivers the results of identity verifications in electronic form to its contract partners and/or to certification service providers for the issuance of qualified electronic certificates. The qualified certificates may then be used to sign legally binding electronic contracts.

Verifeye offers its services to all customers of its contract partners without discrimination.

While the services cannot be provided for people with mutism and deafness, the services provided are accessible for persons with disabilities and can be used without any restrictions by persons with other disabilities.

The services of Verifeye Online have been assessed for compliance with the requirements of eIDAS according to the standards ETSI EN 319 401, ETSI EN 319 411-1, and ETSI EN 319 411-2 and the compliance with the requirements of eIDAS has been confirmed by an independent conformity assessment body.

The video identification services offered by Verifeye Online can be used by Trust Service Providers (TSPs) for the issuance of qualified certificates and qualified seals according to the policies QCP-n, QCP-n-qscd, QCP-l, and QCP-l-qscd of ETSI EN 319 411-2. For QCP-l and QCP-l-qscd Verifeye can only identify the natural person representing the organization, the organization itself must be identified by the TSPs. Also, the affiliation of the natural person and the authorization to act on behalf of the organization cannot be checked by Verifeye; this must be done by the TSPs, if required.

The video identification is performed by trained and experienced identity verification specialists according to legally admitted procedures. The video conference replaces the personal (physical) presence of the person to be identified.

1.2 Document Name and Identification

This document is the “Trust Service Practice Statement” of the Verifeye Online, Sia

Name of the document	Verifeye Online, Sia– Trust Service Practice Statement

Version	2.0
Date	14.01.2026

1.3 PKI Participants

1.3.1 Certification Authorities

A Certification Authority (CA) is an entity authorized to issue public key certificates. A CA is also responsible for the distribution, publication, and revocation of certificates.

Verifeye does not operate a CA but offers identification services on behalf of CAs.

1.3.2 Registration Authorities

A Registration Authority (RA) acts on behalf of a CA. RAs are responsible for verifying both business information and personal data contained in a subscriber's certificate.

An RA submits certificate requests to issuing CAs, approves applications for certificates, renewal, or re-keying, and handles revocation requests.

Verifeye does not operate an RA but offers identification services on behalf of a CAs RA.

1.3.3 Subscribers

Subscribers are the end-entities of certificates issued by a CA. Subscribers are individual persons.

Verifeye identifies the subscribers on behalf of contracted partners or CAs.

1.3.4 Relying Parties

A Relying Party is an individual or entity that relies on a certificate. A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed document and to identify the signer of the document.

1.3.5 Subcontractors

Where the provisioning of services involves subcontracting, outsourcing, or other third-party arrangements, Verifeye Online has documented agreements and contractual relationships in place.

Verifeye Online uses a supplier for the operation of the datacenter. It provides managed dedicated servers for storing data. The operator of the external datacenter is obliged to protect the servers in the datacenter against physical and environmental threats and to maintain the security of the servers in the datacenter up to the operating system level.

The datacenter's conformance with the information security policy is ensured through regular audits performed by Verifeye personnel.

Whereas all external contractors providing video identification services will be subject to respective security requirements and controls as applicable to Verifeye Online (i.e. as described under section 5.1, 5.2 etc.), Verifeye retains overall responsibility for conformance with the procedures specified in its information security policy, even when the specific functionality is undertaken by outsourcers.

1.4 Certificate Usage

Not applicable. Verifeye Online provides identity verification services and does not issue certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This TSPS is administered by:

Verifeye Online, Sia Lāčplēša iela 20A, LV-1011, Riga, Latvia

1.5.2 Contact Person

CEO, Verifeye Online, Sia Lāčplēša iela 20A, LV-1011, Riga, Latvia. E-Email: info@verifeye.online

1.5.3 Person Determining CPS Suitability for the Policy

Verifeye Online's Compliance Officer determines the suitability of this TSPS with the Policy.

1.5.4 TSPS Approval Procedures

This TSPS document has been prepared for compliance with the requirements of eIDAS Chapter III on identity verification for Trust Services.

This Trust Service Practice Statement and amended versions or updates of this TSPS are approved by Verifeye's Senior Management and published and communicated to all relevant employees and external parties immediately.

The Management Board is also responsible for implementing the practices as specified in this document.

The TSPS is reviewed in regular intervals. Amendments to the TSPS and other documents must be approved by Verifeye Online's Senior Management before becoming effective.

Please see www.verifeye.online for details.

Typically, the Terms and Conditions of the certificate issuing TSPs apply. They are made available to all subscribers and relying parties of the TSPs through durable means of communication. Also, the publication of a PKI Disclosure Statement (PDS) is the TSPs responsibility.

1.6 Definitions and Acronyms

1.6.1 Definitions

Not required:

1.6.2 Acronyms

Not required.

1.6.3 References

ETSI EN 319 401	ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319 411-1	ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
eIDAS	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
Vfg Nr. 138/2023	Verlängerung der befristeten Anerkennung der Methode der Videoidentifizierung als „sonstige Identifizierungsmethode“ gemäß § 11 Absatz 1 VDG

2 Publication and Repository Responsibilities

2.1 Repositories

Verifeye Online publishes this TSPS and other relevant documents such as General Terms and Conditions (AGB) and the Data Protection Statement on its website www.verifeye.online

2.2 Publication of Certificate Information

Not applicable. Verifeye does not issue certificates.

2.3 Time or Frequency of Publication

This TSPS and any subsequent amendments are made immediately publicly available after approval. Verifeye develops, implements, enforces, and annually updates this TSPS to meet the compliance standards of the documents listed in Section 1.6.3.

Verifeye Online’s website is publicly available 24 hours per day, 7 days per week. Upon system failure or other kind of outages Verifeye will restore proper functionality without delay.

2.4 Access Controls on Repositories

The repository is publicly and internationally available. Read only access is unrestricted.

Verifeye protects the integrity and authenticity of all documents in the repository. The repository is subject to access control mechanisms to protect its availability and prevent unauthorized persons from adding, deleting, or modifying information in the repository.

3 Identification and Authentication

3.1 Naming

Not applicable. Verifeye does not issue certificates.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Not applicable. Verifeye does not issue certificates.

3.2.2 Authentication of Organization Entity

Not applicable. Verifeye does not issue certificates.

3.2.3 Authentication of Individual Identity

The customer's identity is verified according to eIDAS article 24 (1) letter c) by using "other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body."

The customer's identity is checked against an official, valid, government-issued photo ID document that fulfills legal and regulatory requirements.

The customer has to be present in a video conference call and screenshots and a voice protocol are recorded as evidence.

The information collected during the identification include the full name (surname and given name(s)) of the applicant, the date and place of birth, the current address, the type, validity period, issuing authority, and the reference number of the identity document presented. The current address is either part of the data of the ID document (if contained) or is filled out by the customer before the beginning of the identification process. This information is provided to Verifeye Online via its client's meta api.

Verifeye Online also verifies the customer's mobile phone number for authentication purposes when the customer applies for a qualified certificate at a cooperating TSP (more precisely: CA).

Other aspects beyond the identity of natural persons, e.g. organizational affiliation or authority to act on behalf of someone, must be checked by the TSP who issues the certificate.

After performing the video identification Verifeye Online transfers the collected identification data to the CA.

If the requirements of the RA's national supervisory body go beyond the national requirements for user identity verification applicable to the CA, there is no obligation for the RA to implement such additional requirements for certificate creation for the CA, provided it is ensured that the requirements of the regulations applicable to the CA for the implementation of the identification are met. Insofar the CA will coordinate and address corresponding questions to its supervisory body.

Provided that the

i) correctness of the collected data, and
ii) the comparison of the identity documents used and the applicant

(4-eyes principle) is to be confirmed to the TSP, the RA will carry out this process in agreement with the TSP within 24 hours.

All data exchanged electronically with the customer is protected through encryption. All data included in the transmission to the TSP is encrypted and digitally signed.

3.2.4 Non-verified Subscriber Information

Not applicable. Verifeye Online offers only identity validation services.

3.2.5 Validation of Authority

Not applicable. Verifeye Online offers only identity validation services.

Verifeye Online does not validate the user's authority to apply for a certificate; this must be performed by the CA issuing the certificate.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Not applicable. Verifeye Online does not issue certificates.

Verifeye Online does not differentiate between identifications for initial certificate issuance or re-key requests.

3.4 Identification and Authentication for Revocation Requests

Not applicable. Verifeye Online does not issue certificates and does not handle revocation requests.

4. Certificate Life-Cycle Operational Requirements

Not applicable.

Verifeye Online performs identification services according to chapter 3.2.3. Verifeye Online does not issue certificates, does not process certificate applications, and does not provide certificate status validation services.

5. Facility, Management, and Operational Controls

Verifeye Online carries out regular risk assessments to identify, analyze, and evaluate risks related to its services taking into account business and technical issues.

Verifeye Online then selects appropriate risk treatment measures considering the results of the risk assessment. The risk treatment measures chosen ensure that the level of security is commensurate with the degree of risk.

Verifeye Online has implanted policies and procedures to assess the effectiveness of the risk-management measures.

Verifeye Online's management team approves the risk assessment and accepts the residual risks identified in the risk assessment with this approval.

5.1 Physical Controls

Verifeye Online has implemented a general security policy which supports the security requirements of the services, processes, and procedures covered by this TSPS.

These security mechanisms are commensurate with the level of threat in the identity validation environment.

5.1.1 Site Location and Construction

Verifeye Online operates its platform in the protected environment of a hosting services provider, but fully administered by Verifeye.

For redundancy purposes, Verifeye Online operates its platform in more than one availability zone. Each location is capable to provide the services required for identity verification on behalf of Verifeye.

Verifeye Online's servers are hosted in secure data centers and managed and operated (at the operating system level) by data center staff. The security of the data centers is demonstrated via a suitable certification the existence and validity of which Verifeye regularly checks as part of a compliance assessment.

Several layers of physical security controls restrict access to the sensitive hardware and software systems used for performing

operations. The systems used for identity validation services are placed so that only authorized employees can access them. Verifeye Online's applications and data are stored encrypted and not accessible for data center personnel. The environment is physically protected and deters, prevents and detects unauthorized use of, access to, or disclosure of sensitive information.

5.1.2 Physical Access

Verifeye Online ensures that the area where the identity validations are performed is sufficiently protected against unauthorized access and intrusion through

- an access control system,
- video surveillance and
- automatic alarm facilities.

Verifeye Online ensures that its relevant systems, especially the relevant database servers and the systems used for the identity services, are operated with physical security mechanisms to:

- permit no unauthorized access to the hardware;
- store all identity validation data in encrypted form;
- monitor, either manually or electronically, for unauthorized intrusion at all times;
- maintain and periodically inspect an access log.

Verifeye Online has implemented physical access controls to reduce the risk of unauthorized persons being able to access Verifeye's premises. In addition, Verifeye Online ensures that the physical access to its data centers including database servers, routing and switching components, and firewalls is sufficiently restricted.

All IT components (servers, databases) required for the implementation of the Verifeye Online service are located in specially secured locations. Only administrators have access to the premises in accordance with the principle of dual control, i.e. two persons must authenticate themselves to the secured access points using personalized chip cards and PINs in order to gain access. Every access is logged in a revision-proof manner and regularly analyzed by the Verifeye Online security team.

Visitors to Verifeye Online's premises cannot enter those without support of authorized employees. In all relevant security areas, visitors must be accompanied by authorized employees.

5.1.3 Power and Air Conditioning

All systems at the locations where identity verification takes place and all systems in the secure data center have industry standard power and air conditioning systems to provide a suitable operating environment.

Furthermore, all relevant systems are provided with an uninterruptable power supply sufficient for a short period of operation in the absence of commercial power, to support either a smooth shutdown or to re-establish commercial power.

5.1.4 Water Exposure

The secure data centers have reasonable precautions taken to minimize the impact of water exposure.

5.1.5 Fire Prevention and Protection

The secure data centers have industry standard fire prevention and protection mechanisms in place.

5.1.6 Media Storage

All storage media is managed through all life cycle phases acquisition, use, transportation and disposal in accordance with Verifeye's classification scheme and handling requirements.

Sensitive physical media is stored in a safe to protect it from accidental damage (such as water, fire, electromagnetic fields, etc.) and damage, theft, unauthorized access, obsolescence and deterioration. Media that contains audit data, archive data, or backup information is duplicated and stored securely as described in section 5.1.2.

All data carriers used are encrypted when data is stored on them. Only Verifeye Online is in possession of the keys needed to decrypt such encrypted data. Paper-based information is securely destroyed via a service provider.

5.1.7 Waste Disposal

Most sensitive documents and materials occur only in electronic form. Media used to collect or transmit sensitive information are securely erased before disposal. Non-functional data carriers where erasing is not possible are physically destroyed before disposal.

Paper-based media with critical information is disposed in such a way, that the restoration of the information is prevented by using a shredder. Other waste is disposed of in accordance with normal waste disposal requirements.

5.1.8 Off-site backup

Verifeye Online performs regular routine backups of critical system data, audit log data, and other sensitive information.

Verifeye Online stores identity verification data only for a short period of time. All relevant identity verification data is sent to the Qualified Trust Service Provider (QTSP) immediately after being collected for the purpose of issuing a qualified certificate. The QTSP is then obliged to archive these data according to the regulations made in eIDAS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted persons include all employees that have access to the source code or administer the Verifeye Online platform or perform identifications.

Personnel in trusted roles is named and approved by senior management of Verifeye Online. Persons in trusted roles must accept and agree to this assignment of a trusted role.

Special roles include:

Security Team

The security team consists of a Chief Information Security Officer (CISO) and several security experts like System Auditors, checking archives and audit logs.

In addition to developing personnel, organizational, technical and infrastructural security measures, the security team is also responsible for implementing these measures and maintaining them during ongoing operations. This requires not only regular training of all Verifeye Online employees, but also adjustments to the current security situation in order to be able to react to any security incidents that may occur.
At least one person is identified as responsible for network and information security. This person is also responsible for reporting to top management.

System Administration Team

Verifeye Online has appointed an Administration Team which consists of System Administrators (install, configure, maintain and recover systems) and System Operators (operate the systems and perform system backups of it).

Data Protection Officer (DSB)

In line with the European Commission's new basic data protection regulation, Verifeye Online has appointed a Data Protection Officer. The data protection officer is not only sup- ported by a team of qualified employees, but also by

renowned scientific institutions. With respect to data security, the Privacy Team works closely with the Verifeye Security Team.

Chief Information Security Officer

Verifeye Online has appointed a Chief Information Security Officer (CISO). Its main tasks include:

- Coordination of information security goals with the company management
- Coordination and planning of information security in cooperation with the Information Security Team (IST)
- Creation and maintenance of guidelines and regulations for information security in the company
- Advising management on information security issues
- Documentation of information security measures
- Information security training for employees
- Planning and design of incident management ("Incidents") and emergency precautions (incl. emergency plan/manual)

Compliance Officer

Verifeye Online has appointed a Compliance Officer. The Compliance Officer implements the compliance regulations of Verifeye Online in the corporate structure and business processes by setting up a compliance management system. With his knowledge of the corporate structure as well as the operational processes and products, he determines the company-specific risks for legal violations in a systematic risk analysis.

Verification Specialist

Verification Specialists (or Identity Verification Agents) partly assume the TSP role of an RA Officer. They are responsible for the remote identification of persons in video sessions,

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

Initially, the identity of all personnel in trusted roles is verified through personal, physical presence and the check of an official photo ID document. Identity is further confirmed through the background checking procedures in section 5.3.2.

Personnel have no access to the trusted functions until the necessary checks are completed.

Personnel in trusted roles is approved by senior management of Verifeye Online before being permitted to perform the functions of the trusted role, i.e. perform identity validations or access relevant systems.

The principle of "least privilege" applies whenever access to relevant systems is required or when access privileges are configured.

Verifeye ensures that users are authenticated by multi-factor mechanisms, such as individual passwords and individual access tokens and PINs, before accessing Verifeye's systems or network.

5.2.4 Roles Requiring Separation of Duties

All personnel performing sensitive operations are assigned a trusted role. A segregation of conflicting duties and areas of responsibility is implemented to reduce opportunities for modification and misuse to its minimum.

5.3 Personnel Controls

In addition to Verifeye Online, the requirements from chapter 5.3 also apply to external service providers and the outsourcing partners.

5.3.1 Qualification, Experience, and Clearance Requirements

All employees involved in the operation of Verifeye Online's systems have appropriate knowledge and experience related to their duties. They must have demonstrated security consciousness and awareness regarding their duties and receive appropriate training in organizational policies and procedures.

Employees involved in identity verification services have signed a confidentiality (non- disclosure) agreement as part of their initial terms and conditions of employment.

Managerial personnel possess professional experience with the services provided and are familiar with security procedures for personnel with security responsibilities.

Personnel in trusted roles are held free from conflict of interest that might prejudice the impartiality of operations.

5.3.2 Background Check Procedures

All employees of Verifeye Online are thoroughly checked for their qualifications for the tasks for which they are responsible before being hired. Training and previous employment are examined on the basis of training and work certificates.

In addition, new employees undergo a criminal background check prior to officially joining Verifeye Online. The checks must be clear of records related to trustworthiness.

Regular periodic reviews of background checks are performed as far as permitted by Latvian law to verify the continuous trustworthiness of all personnel.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the Verifeye Online systems and services receive comprehensive training. Training is conducted in the following areas:

- Information Security,
- Compliance,
- Data Protection,
- Relevant norms and standards,
- Security principles and mechanisms,
- Use and operation of the Verifeye Online platform,
- Incident handling and reporting,
- Disaster recovery procedures.

Verifeye Online conducts regular security training sessions to raise awareness of Information Security and Data Protection. Training is mandatory not only for Verifeye's technical staff (e.g. system administrators and developers), but also for administrative staff, the verification agents and for the respective target groups. The courses cover all relevant topics of Information Security and Data Protection, from current threats to attacker procedures (including social engineering) to the consequences of successful attacks and methods for risk minimization.

In addition, renowned researchers are invited to present current topics from their work and discuss their results at internal knowledge days. The insight into innovative technologies allows the continuous improvement of Verifeye Online.

Verifeye Online maintains records of compliance, Data Privacy, security trainings and identity verification specialist training performed.

5.3.4 Re-Training Frequency and Requirements

Retraining is performed to the extent and frequency required to ensure that the required level of proficiency is maintained. This includes regular (at least quarterly updates on new threats and current security practices.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions are taken in case of unauthorized actions (i.e., not permitted by this TSPS or other policies). A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures.

5.3.7 Independent Contractor Requirements

Not applicable. Verifeye Online does not use Independent Contractors.

5.3.8 Documentation Supplied to Personnel

This TSPS, Verifeye Online's Information Security Policy, applicable system operations documents, operations procedures documents, reference material for ID documents and any relevant other documents required to perform their jobs have been made available to Verifeye Online's employees. This includes the verification specialists.

5.4 Audit Logging Procedures

In addition to Verifeye Online, the requirements of chapter 5.4 also apply to external service providers and the outsourcing partners.

5.4.1 Types of Events Logged

Verifeye Online keeps audit trails and system log files that document actions taken as part of the identity verification services.

All relevant events related to the services provided are logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.

Security log entries include the following elements:

- date and time of the entry
- description/kind of entry.

The security logs are automatically collected.

The identity verification audit logs include:

- date and time of the entry,
- kind of identification methods used,
- type of document(s) presented by the applicant to support registration,
- reference to the identity of the person performing the identity proofing.

These audit logs are automatically created, integrity protected and immediately encrypted. They can only be accessed in case of a special audit using a distinct auditor decryption key.

5.4.2 Frequency of Processing Log

Verifeye Online's system and its components are continuously monitored and capable of providing real time alerts if unusual security and operational events occur and allow an immediate review by system security administrators.

The security logs are regularly reviewed including verification that the logs have not been tampered with. Any alerts or irregularities detected in the logs are investigated. Actions taken based on security log reviews and alerts are documented.

5.4.3 Retention Period for Audit Log

Event logs are stored for 10 years in minimum. Records are archived for as long as required by the respective legislation and specific regulations.

5.4.4 Protection of Audit Log

Procedures are implemented to protect archived data and audit data from destruction or modification prior to the end of the audit log retention period. Audit logs are moved to a safe, secure storage location separate from the component which produced the log (dedicated log server).

Access to audit logs is restricted to authorized personnel.

5.4.5 Audit Log Backup Procedures

Audit logs are stored within the data centers which provide sufficient redundancy via its availability zone concept and the geographically distinct locations.

5.4.6 Audit Collection System (Internal vs. External)

Audit data is generated and recorded automatically at the application, network, and operating system level. Audit logs are then transmitted to a dedicated log server.

5.4.7 Notification to Event-Causing Subject

No stipulation

5.5 Records Archival

The requirements of chapter 5.5 also apply to external service providers and outsourcing partners.

5.5.1 Types of Records Archived

At a minimum, Verifeye Online records the following data for archival:

- this TSPS
- contractual obligations
- system and equipment configuration
- modifications and updates to systems or configurations
- audit logs mentioned in section 5.4
- documentation required by compliance auditors.

5.5.2 Retention Period for Archive

All records are archived in accordance with legal or regulatory requirements. For supporting information, this is usually for at least ten years.

Long term archival of such evidences collected during identifications and supporting information, i.e. identification data according to the requirements of eIDAS, is regulated by contractual agreements with the QTSP.

Either the QTSP is responsible for archival of identification data and contractually agrees with Verifeye Online on a shorter archive period specified in the contractual agreements or the QTSP contractually agrees with Verifeye Online that long-time archival is in the responsibility of Verifeye. In this case the archival period is specified in the contracts with the QTSP.

In any case, in accordance with data protection regulation, all person-related data is deleted from Verifeye Online's systems after the archive period has expired.

5.5.3 Protection of Archive

Verifeye Online protects the archive so that only authorized persons in trusted roles can access the archive. The archive is stored in a trustworthy system protecting it against unauthorized viewing, modification, deletion, or other tampering. The media holding the archive data and the applications required to process the archived data is maintained to ensure that the archive data can be accessed for the time period defined in chapter 5.5.2.

5.5.4 Archive Backup Procedures

Verifeye Online performs regular database backups according to Verifeye's backup concept. This concept considers the criticality of the data and defines the minimum backup cycles and backup methods.

In order to ensure the availability and readability of backups the procedures for recovery are regularly tested.

The backups are performed by the administrators. The CISO is responsible for the correct execution of the backup.

5.5.5 Requirements for Time Stamping of Records

Time stamping of records is not required.

5.5.6 Archive Collection System (Internal or External)

The archive collection systems are internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Access to the archive is restricted to personnel in trusted roles.

Information in the archive is verified in regular intervals as described in section 5.4.2.

5.6 Key Changeover

Not applicable. Verifeye Online does not handle CA keys.

5.7 Compromise and Disaster Recovery

Verifeye Online has implemented a disaster recovery and business continuity plan intended to allow restoration of business operations in a reasonably timely manner following interruption to, or failure of, critical business processes.

Based on mobile communication and VPN-based use of internal IT-systems and data, Verifeye Online employees can work in a decentralized manner from different locations and even from home until the availability of the primary location is restored or a contingent location ready for use.

This does not apply to identity verifications; identity verifications must be performed in the dedicated office of Verifeye Online.

In addition to Verifeye Online, the requirements from chapter 5.7 also apply to external service provider and the outsourcing

partner.

5.7.1 Incident and Compromise Handling Procedures

Should security gaps become apparent, e.g. due to own observations or actual attacks, the security team has already conducted possible attack scenarios and prepared appropriate countermeasures. These can range from the short-term shutdown of security- critical services to the shutdown of the entire platform until security is restored.

In addition, the current security situation is regularly monitored. Other sources, e.g. the Computer Emergency Response Team of the Federal Office for Information Security, provide information on current security gaps and attacks to initiate appropriate countermeasures.

The regular internal procedures of the departments and internally responsible contact persons are used to deal with security incidents. Verifeye's Board and management team are informed and involved in a supportive manner if necessary.

Verifeye Online addresses any critical vulnerability not previously addressed, within 48 hours of its discovery.

Incidents affecting the security or the integrity of Verifeye Online's services are reported to the relevant CA(s) and to the supervising authority, and, if applicable, to affected subscribers and third parties, without unnecessary delay (in any case within 24 hours) after Verifeye Online has become aware of the incident by the required means of communication.

Reporting procedures are implemented which may be used by Verifeye staff, contractors and customers by submitting incident reports via e-mail or Verifeye's intranet. These reporting procedures are communicated to contractors and customers.

Verifeye personnel is trained to follow the reporting procedures and to address incident reports to the suitable recipients. Hence, Verifeye Online ensures that relevant incidents are reported in-line with Verifeye Online's procedures. Roles, responsibilities and procedures involved in incident handling are reviewed and tested in regular intervals and, in addition, after each incident that occurred.
Verifeye Online documents all relevant security incidents, including information about the incident detection and the response process. After any incident Verifeye Online will start an examination of the incident, identify the root cause(s) of the incident and conduct a post-incident review. This might result in the creation of additional measures mitigating the risk of recurrence of similar incidents.

In order to distinguish between incident handling and business continuity management functions Verifeye Online has created clear interfaces separating incident handling from business continuity. This separation allows coordinated and cohesive responses during incidents.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

Verifeye Online maintains backup copies of its databases and software to be able to rebuild business capabilities in case of software and/or data corruption.

In the event of corruption of computing resources, software, and/or data employees immediately report such an occurrence to the security team. The security team invokes the emergency plan if required.

If software or data has been corrupted the affected system is completely wiped to remove any possible remaining causes for the corruption. The system is then restored in a clean manner.

5.7.3 Entity Private Key Compromise Procedures

Not applicable. Key compromise must be handled by the QTSP.

5.7.4 Business Continuity Capabilities after a Disaster

Business Continuity Management (BCM) protects Verifeye Online in an emergency from serious damage or losses threatening its existence. This also applies to external service providers. It describes the content, personnel and organizational specifications and procedures for emergency management to

- ensure the continuation of time-critical activities and processes should an emergency occur
- take appropriate measures to avoid damage as far as possible
- to reduce the impact of damage that has occurred
- support a fast and orderly restoration of normal operation

The person responsible for Verifeye Online in case of emergencies is named, the definition of the terms as well as the processes according to Plan - Do - Check - Act takes place. The emergency manual describes the emergency strategies considering defined emergency scenarios and their criticality. Specifications and details are described in the "Business Continuity Management" guideline.

Verifeye Online has created and maintains a business continuity plan so that in the event of a business disruption critical business functions may be resumed.

In the event of a disaster requiring permanent cessation of operations from the primary facility, Verifeye Online's management will assess the situation and formally declare a disaster situation, if required.

Once a disaster situation is declared, the restoration of services functionality at a secondary site will be initiated. The Operator of the Verifeye Online IT Services is contractually obligated to make the services available at a secondary site in less than 12 hours after a disaster.

After a disaster has been dealt with, the CISO analyses the causes and takes measures according to the ISO 27000 process to prevent a recurrence of the incident.

Verifeye Online conducts regular disaster recovery and business continuity tests to ensure functionality of services in the case of a disaster.

5.8 CA or RA Termination

Not applicable. Verifeye Online does not operate a CA or RA Services.

5.8.1 Termination of Identification Service

Verifeye Online has implemented a termination plan that defines which actions must be taken in case of termination of services. Among others, the termination plan covers the aspects which entities must be informed about the termination, to whom remaining obligations will be transferred, and who will store relevant data that needs to be retained.

As after termination of services no systems are required to be operational for a longer period Verifeye Online will bear the costs for the execution of the termination plan.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Not applicable. Verifeye Online does not generate keys for CAs or PKI customers.

Verifeye Online generates keys only for its own, internal purposes and for securing the communication with persons to be identified.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Not applicable for cryptographic module engineering controls because Verifeye Online does not operate cryptographic modules.

Verifeye Online manages only private keys for its own purposes, for encrypting the applications and data stored on the servers in the third-party datacenter.

For encrypting the communication with the TSP, the TSP has provided a 2048 bit encryption key. Identification data is encrypted with a randomly chosen AES key, the AES key is then encrypted with the public part of the 2048-bit encryption key. Encrypted key and encrypted data are then sent to the TSP.

Verifeye Online keeps the number of personnel authorized to use these keys to a minimum. Unauthorized use is prohibited. The passphrases for these keys are kept secret.

6.3 Other Aspects of Key Pair Management

Not applicable. No special key management procedures like dual control are considered necessary. In particular, Verifeye Online does not generate and manage keys on behalf of other parties.

6.4 Activation Data

Not applicable. Verifeye Online does not manage keys or cryptographic devices where activation data needs special protection.

6.5 Computer Security Controls

A general information security policy document (information security policy) is available and has been approved by management. It is published, and communicated, as applicable, to all employees, contract partners, assessment bodies, supervisory or other regulatory bodies affected by it. The information security policy may be supplemented by detailed policies and procedures for personnel involved in specific functions, e.g. identity verification or system administration or network management.

The information security policy contains a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing. It contains a statement of management intent, supporting the goals and principles of information security, and explains the security policies, principles, standards, and compliance requirements of particular importance to the organization.

The information security policy lists general and specific responsibilities for information security management, including reporting security incidents, and contains references to documentation which supports the policy. Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined. An authorization process for new software releases or information processing facilities exists and is followed.

Verifeye Online's management ensures that there is clear direction and visible management support for security initiatives. Verifeye's management is responsible for maintaining the information security policy and coordinates the implementation of information security measures. This includes regular reviews (at least yearly) of the information security policy and associated documents like the risk assessment, the inventory of assets, and the TSPS.

The information security policy, the risk assessment and other policies are approved by Verifeye Online's management, reviewed regularly (at least yearly) and revised if necessary. In particular, the management accepts with the approval of the risk assessment the residual risks related to the provision of its (identity validation) services.

6.5.1 Specific Computer Security Technical Requirements

All statements of this section apply not only to Verifeye Online's systems; they apply to External Identification Centers as well.

Verifeye Online ensures that the systems storing and processing software and data are trustworthy systems protected against unauthorized access.

All systems are protected against viruses, malicious, and unauthorized software.

Patches or updates for network security software components or operating system components are applied within a reasonable time after their relevance and applicability has been verified. Reasons for not applying security patches are documented.

All systems are hardened, i.e. all unnecessary user accounts, applications, protocols, and ports are removed or disabled.

Access to systems is restricted to individuals with a valid business reason for such access. General application users have no accounts on production systems. The access control policy applies. User and account management has been implemented. Access rights are granted based on the role concept and the need-to-know principle; the principle of least privilege is applied for all roles. Rights are immediately removed if no longer required. In addition, user accounts, roles, and access rights are regularly reviewed. Particularly, use of system utility programs is restricted and controlled.

All data is stored in encrypted form to protect it against manipulations and unauthorized access.

The network with systems for identity verification is logically separated from other components. This separation prevents network access to critical systems except through defined application processes and network paths. Firewalls are installed to protect the production and management network from internal and external intrusion or other forms of attacks.

Direct access to databases supporting identity verifications and storing customer's identity data is limited to persons in Trusted Roles having a valid business reason for such access.

The workplaces of the identity verification specialists must be physically separated from each other in such a way that the video cameras and microphones of one workplace cannot capture screen images or voices of video conferences at other workplaces. Workplaces are configured with minimum application set-up and user account access rights are restricted to those rights which are necessary for operating the identification process.

Bringing personal belongings (e.g. smartphones) to the identity verification workplaces is prohibited.

6.5.2 Computer Security Rating

The use of evaluated components is not required.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Development systems are separated from production systems.

New software or new applications, releases, modifications and emergency software fixes are installed on production systems only after they have been successfully tested according to the change control policy. Installation of new software or applications prior to approval is not permitted.

6.6.2 Security Management Controls

The configuration of Verifeye Online's systems and any modifications and upgrades must be documented and controlled.

Verifeye Online's information security management system is ISO 27001 certified. It ensures that proper security controls adequate to manage the risks are implemented.

6.6.3 Life Cycle Security Controls

Not applicable for Verifeye Online's hardware.

In order to support the trustworthiness of the systems a procurement process for hard- and software is followed. The PCs and servers are commercial off-the-shelf products; there are no special technical requirements that need to be fulfilled.

Identity verification system development is done in Verifeye's development environment, development personnel undergo background checks before employment.

System configuration is managed through change control mechanisms. Security management controls are applied to ensure that the operational systems and networks adhere to configured security. This includes checking the integrity of the software applications, firmware, and hardware to ensure their correct operation.

6.6.4 Network security controls

Verifeye has separated its network into different zones. It uses separate dedicated networks for the administration of its operational IT systems (e.g. databases) and the video identification clients. The communication between the IT systems and zones is limited to the necessary communication regarding the identification process.

Systems used for the administration of the security policy implementation are not used for other purposes. All systems relating to the identification process are co-located in the same zone. The same security controls apply for all systems co-located in the same security zone. For example the change control procedures, hardening measures and patching procedures are identical for all systems in the same zone.

Verifeye Online has installed adequate protection from both inside and outside attacks (firewalls, intrusion detection mechanisms, etc.).

Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy.

Configurations of servers, clients, and all network routing systems including firewalls are regularly checked for compliance with the requirements of this TSPS.

Access to all servers is subject to authentication.

Communication of sensitive information, especially the video conference stream and the identification data submitted to the CA, is always protected through encryption.

Vulnerability assessments:

Software may have errors. Some of these errors can lead to security vulnerabilities. The same applies to the security measures implemented, be they of personnel, organizational, technical or infrastructural nature. Despite evaluation of these measures regarding security, security gaps may arise which were not identified in the evaluation.

The security team therefore regularly checks the effectiveness of the implemented measures, also by simulating its own attacks (hacking, but also e.g. phishing attacks), and thus tests the effectiveness of the security measures and security training courses. In addition, based on events in the log files the security team initiates vulnerability assessments.

Vulnerability scans are performed by persons or entities with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

Vulnerability scans are performed by Verifeye Online monthly or on an ad hoc basis, for example after relevant changes.

Penetration tests:

Penetration tests are performed on a yearly basis by an independent third party with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report for all of Verifeye Online's network components and systems; additional tests are carried out insofar as safety-relevant changes have been made.

For any vulnerability found during such vulnerability scans or penetration tests Verifeye Online

- creates and implements a plan to mitigate the vulnerability; or
- documents the factual basis that the vulnerability does not require remediation.

6.7 Time stamping

Cryptographic time stamps are not required.

However, database entries about identification sessions contain time and date information. File names of protocols and other relevant records like log files must include at least the date of creation.

Systems synchronize their internal time via NTP protocol. Verifeye Online's NTP daemon synchronizes with the public services of the Open Telekom Cloud (OTC) and is installed on the production machines.

7 Certificate, CRL, and OCSP Profiles

Not applicable. Verifeye does not issue certificates or CRLs and does not operate OCSP responders.

8 Compliance Audit and Other Assessments

Verifeye Online is subject to regular external assessments. These include assessments pursuant to ETSI EN 319 401, 319 411-1 and 319 411-2 which are required to prove conformity with the regulations made in eIDAS Chapter III.

Verifeye Online will inform the supervisory body at the latest one month before any planned compliance assessment and will allow the supervisory body to participate as an observer upon request.

These assessments require demonstration of a maximum level of security and conformity to well recognized policies and practices.

In addition, Verifeye Online performs internal self-assessments. Topics covered by these assessments include checks of proper implementation of applicable policies and extensive checks on the quality of identifications performed and on the quality of collected evidences collected during identifications.

The results of these compliance assessments are documented and archived. They may be released at the discretion of Verifeye Online management to compliance auditors and if required by government authorities for the purpose of legal proceedings.

8.1 Frequency and Circumstances of Assessment

According to eIDAS, article 20 (1) compliance audits according to section 8 must be performed at least every 24 months. Surveillance audits are made 12 months after each full audit.

Additional assessments are required if substantial changes are made to Verifeye Online's systems, configurations, or processes that might affect the overall security if the services. Verifeye Online will inform the Latvian supervisory body and the qualified trust service providers for which Verifeye Online provides its services about such substantial changes at least one month before the changes are implemented.

8.2 Identity/Qualifications of Assessor

The conformity assessment required by eIDAS is performed by an accredited assessment body.

8.3 Assessor's Relationship to Assessed Entity

Compliance assessments must be performed by a Conformity Assessment Body (CAB) that is accredited to operate under eIDAS and that is independent of Verifeye Online.

8.4 Topics Covered by Assessment

The purpose of a compliance audit is to verify that Verifeye Online's components comply with the statements of this TSPS, with the eIDAS regulation, and with the requirements specified in the audit standard under consideration.

Thus, all applicable aspects of this TSPS and all the standards mentioned in section 8 are covered by the compliance audits.

The scope of the ETSI audit includes (but is not limited to) environmental controls, infrastructure and administrative CA controls, network controls, and identity verification processes and procedures.

8.5 Actions Taken as a Result of Deficiency

If significant exceptions or deficiencies are identified during the compliance audit as defined in section 8 this will result in a determination of actions to be taken. This determination will be made by Verifeye Online's management in cooperation with the auditor. Verifeye Online's management in collaboration with the Conformity Assessment Body is responsible for

developing and implementing a corrective action plan.

If it is determined that such exceptions or deficiencies pose an immediate threat to the identity verification services a corrective action plan must be developed within a period of time agreed upon with the evaluator and implemented within a reasonable period of time. For less serious exceptions or deficiencies, the management evaluates the significance of such issues and determines the appropriate actions.

8.6 Communications of Results

The resulting conformity assessment report is submitted to the Latvian supervisory body within three working days of receipt.

9 Other Business and Legal Matters

9.1 Fees

Fees for the identity verification services are subject to contractual agreements between Verifeye Online and its business partners.

Verifeye Online does not charge a fee for access to this TSPS. Any use other than viewing, such as reproduction, redistribution, modification, or creating derivatives is not permitted.

9.2 Financial Responsibility

For both contractual and non-contractual users and business partners the regulations of indemnification of Latvian law are binding.

Verifeye Online undergoes regular financial assessments to verify that it has the financial stability and resources required to operate in conformity with this TSPS and the requirements of eIDAS.

9.2.1 Insurance Coverage

Verifeye Online maintains a Professional Liability insurance coverage.

9.2.2 Other Assets

No stipulation.

9.3 Confidentiality of Business Information

In addition to Verifeye Online, the requirements of chapter 9.3 also apply to external service provider and outsourcing partner.

9.3.1 Scope of Confidential Information

In the framework of the established, ISO 27001 certified information security management system (ISMS), the level of confidentiality of information is determined. Four levels of confidentiality are distinguished: public, internal, confidential and strictly confidential. (Strictly) confidential information include in particular any information provided by user for purposes of identity verification.

9.3.2 Information Not Within the Scope of Confidential Information

Documents and other information classified within the ISMS classification scheme as public are not considered confidential/ private information.

9.3.3 Responsibility to Protect Confidential Information

All of Verifeye Online's personnel are responsible for protecting the confidential information in their possession in accordance with this TSPS, in accordance with contractual agreements, and in accordance with the German data protection regulations.

9.4 Privacy of personal information

9.4.1 Privacy Plan

All information that allows the identification of users is protected from unauthorized dis- closure.

9.4.2 Information Treated as Private

Latvian statutory data privacy law defines which information must be treated as private. Further information to be treated as private can be contractually agreed upon.

9.4.3 Information not Deemed Private

Information included in the certificates that are issued by a CA based on identity verifications performed by Verifeye Online is considered not to be private.

9.4.4 Responsibility to Protect Private Information

All employees of Verifeye Online receiving private information are obliged to protect it from compromise and disclosure to third parties.

All employees must adhere to Latvian and European privacy laws.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this TSPS Verifeye Online will not use private information without the owner's consent.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

If disclosure of private information about users is necessary in response to judicial, administrative, or other legal proceedings the information shall be given only to the requesting authority or the users themselves.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Not applicable.

9.6.2 RA Representations and Warranties

Verifeye Online has overall responsibility for all technical and organizational processes and procedures of its identification services.

Verifeye Online warrants that it performs identity verification functions as described in this TSPS.

Verifeye Online forwards complete, accurate, and verified data about subjects for further processing and issuing qualified certificates to the CA.

Retention, archiving, and protection of data are performed according to the stipulations of this TSPS.

Archived subscriber data is protected in compliance with Latvian and European data protection legislation, all data is stored in encrypted form.

Technical services may be performed by reliable third-party data center personnel. Data center personnel have no access to data collected during identity validations.

9.6.3 Subscriber Representations and Warranties

Not Applicable. Verifeye has no subscribers because it does not issue certificates.

9.6.4 Relying Party Representations and Warranties

Not applicable. Verifeye Online does not issue certificates and has no contact with relying parties.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

Limitations of Liability are subject to contractual agreements between Verifeye Online and its business partners. In any case, limitations of liability contained in Verifeye Online's General Terms of Use (available at https://Verifeye Online.de/en/terms-of-use-for-customers/) shall apply. Limitations of Liability as specifically agreed on in each individual case, where applicable, remain unaffected.

Verifeye Online is legally liable for all vicarious agents and subcontractors as for its own actions. Furthermore, Verifeye Online ensures that all vicarious agents and subcontractors used are sufficiently liable to Verifeye Online in accordance with the risk involved. In accordance with the Supplier and Service Provider Policy, it is mandatory to include certain contents or security clauses for the contracts with the provider. The contracts must also take into account the results of risk assessments. Furthermore, the following aspects must be specified:

Definition of the information to be protected; measures and obligations to protect the information (e.g. e-mail encryption) and dealing with security incidents and breaches of the agreement.

9.9 Indemnities

The regulations of indemnification of Latvian law are binding.

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, users and CAs issuing qualified certificates based on the identity verification

performed by Verifeye Online may be required to indemnify Verifeye for:

- submitting false facts or misrepresenting facts on the user's identity,
- failure to disclose a material fact on the identity verification with intent to deceive any party,
- failure to protect the user's private data, use of an untrusted system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the user's private data.

9.10 Term and Termination

9.10.1 Term

The TSPS becomes effective upon publication on Verifeye Online's web site. Amendments to this TSPS become effective upon publication.

9.10.2 Termination

This TSPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Despite the fact that this TSPS may eventually no longer be in effect, the following obligations and limitations of this TSPS shall survive section 9.6 (Representations and Warranties), section 9.2 (Financial Responsibility), and section 9.3 (Confidentiality of Business Information).

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this TSPS may be made by Verifeye Online's management. Amendments shall either be in the form of a document containing an amended form of the TSPS or an update. Amended versions or updates shall be published in the repository.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

For disputes with end-users and relying parties the dispute resolution procedures of the issuing QTSPs apply.

Complaints regarding Verifeye Online's services can be submitted to complaints@Verifeye Online.com.

As a licensed payment service provider, Verifeye Online is obliged to maintain a complaint management process for consumers according to the guidelines JC 2014 43 27 of the Joint Committee of the European Supervision Authorities. Verifeye has extended the scope of this complaint process also to all customer complaints under the field of application of this TSPS.

9.14 Governing Law

Applicable law is the law of the Federal Republic of Latvia.

9.15 Compliance with Applicable Law

This TSPS is subject to applicable Latvian law, in particular the eIDAS regulation and the "Vertrauensdienstegesetz" (VDG) implementing the eIDAS regulation in Latvia.

This TSPS is compliant to the German Vfg Nr. 138/2023, Verlängerung der befristeten Anerkennung der Methode der Videoidentifizierung als „sonstige Identifizierungsmethode" gemäß § 11 Absatz 1 VDG which authorizes Verifeye to offer its services of video identification as a module for identity verification as an alternative identification method according to eIDAS article 24.

Verifeye Online has created appropriate policies and corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of identity proofing services, including at least measures related to the following:

(i) registration and on-boarding procedures for a service;
(ii) procedural or administrative checks;
(iii) the management and implementation of services;

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If parts of any of the provisions in this TSPS are incorrect or invalid, this shall not affect the validity of the remaining provisions until the TSPS is updated. The process for updating this TSPS is described in section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

Verifeye Online shall not be responsible for any breach of warranty, delay, or failure in performance under this TSPS that result from events beyond its control, such as strike, acts of war, riots, epidemics, power outages, fire, earthquakes, and other disasters.

9.17 Other provisions: Obligation of Service Provider

According to Verifeye Online's policy for suppliers and service providers, the obligations and responsibilities of the service providers and subcontractors used must be precisely defined. Furthermore, all service contracts must contain the following content:

- Rules on the confidential handling and exchange of data and information.
- Return of company assets.
- Rules on the admissibility of subcontracting.
- Reliable delivery of products.
- Service level (SLA).
- Dealing with security incidents and breaches of agreement.
- Ownership of values.
- Measures to protect information.
- Definition of the information to be protected.
- Audit rights of Verifeye Online.
- The service provider shall establish and maintain a set of rules for their task.
- The service provider is organizationally and technically capable of performing their tasks in compliance with the following set of rules:
    - all applicable ETSI norms which are relevant for the provision of the service under consideration. In particular, compliance with the requirements of ETSI EN 319401 and ETSI EN 319411-1/2. Compliance with ISO 27001 if applicable.
    - legal requirements like eIDAS and NIS2 as far as possible.
- The service provider has sufficient resources to perform its tasks and, if necessary, to assume the liability arising from the tasks.
- If the service provider uses external third parties (subcontractors) to perform the assigned tasks, these third parties must be known to Verifeye Online and must have at least the same level of trust as the body.
- If a license is required to provide the service, this must be verified.

10 Document Maintenance

Document Name:	Verifeye Trust Services Practice Statement
Language:	English
English Title:	Verifeye Trust Services Practice Statement
Translation:	
Classification:	Public
Category (Level):	
Authors:	Christopher Gray and Samy Patel
Contact:	Christopher Gray
Date of entry into force:	14 January 2025
Last Review:	14 January 2026
Next Review:	TBD

11 Document History

Version	Date	Responsible	Reason for Change
0.1	26.05.2024	Christopher Gray	Document created
0.2	30.05.2024	Christopher Gray	Completion of initial draft
0.3	10.06.2024	Bernd Kirsig	Review
0.4	16.06.2024	Christopher Gray	Review
0.5	26.06.2024	Bernd Kirsig	Improvements
1.0	14.01.2025	Christopher Gray	Release Version
2.0	14.01.2026	Christopher Gray	Release Version