PXL Vision Identity Proofing Service Practice Statement for PXL Ident

1 Introduction

PXL Vision is an identity service provider offering digital identity verification services in order to support PXL Vision's customers needing reliable identification of their users.

In addition, PXL Vision enables individual users of the contracted customers in collaboration with qualified trust service providers and contract partners to electronically sign documents using qualified electronic signatures according to the eIDAS and ZertES regulations.

The identity verification service PXL Ident is compliant with ETSI TS 119 461 for the use cases

- unattended remote ID proofing hybrid manual & automated operation (9.2.3.3) and
- unattended remote ID proofing automated operation (9.2.3.4);

as well as regulation No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions (eIDAS) and the Swiss Federal Act on the Electronic Signature SR 943.03, (ZertES). In particular, PXL Vision verifies the identities of natural persons in accordance with eIDAS, Article 24, paragraph 1 d) by using "other identification methods" which provide equivalent assurance in terms of reliability to physical presence.

This document is the IPSPS of PXL Vision AG. It is not a full CPS according to RFC 3647, because PXL Vision only provides identity verification services and does not offer other trust services like the issuing of certificates or the provisioning of certificate validation services.

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

1.1 Overview

PXL Vision's services allow users of our customers to be reliably identified using an automated, AI-based identification and hybrid methods while the user is not physically present. PXL Vision delivers the results of identity verifications in electronic form to its customers and/or to trust service providers for the issuance of qualified electronic certificates. The qualified certificates may then be used to sign legally binding electronic documents, e.g., contracts.

The PXL Vision product PXL Ident is a web application, which is accessible via the Internet and can be used in a web browser. It offers the full identity verification functionality.

PXL Vision services are offered to all users of our customers without discrimination. One of the main focuses of PXL Vision is to provide products that can be used by any person, independent of technical capabilities, age or other factors. Even though the strongest value of the services provided by PXL are heavily based on advanced technology, PXL Vision's goal is to make the technology together with its services available and usable by every person that needs to verify their identity.

PXL Vision's identification services as described in this document conform to the eIDAS and ZertES regulations on electronic identification, certification and trust services. They have been assessed for compliance with the relevant requirements of eIDAS and ZertES according to the standards ETSI EN 319 401 and ETSI TS 119 461 and the compliance has been confirmed by an accredited conformity assessment body (CAB).

This IPSPS applies to Identification Services for the following trust service policies:

- EN 319411-1 LCP,
- EN 319411-1 NCP, and
- EN 319411-2 QCP-n

Terms of use apply as displayed to the subscriber as part of the process.

1.2 Document Name and Identification

- This Document's Name: PXL Vision Identity Proofing Service Practice Statement - PXL Ident
- This Document's Owner: PXL Vision AG
- This Document's Version: V1.0
- This Document's Release Date: Jan. 20, 2025

1.3 PKI

The following participants are relevant:

1.3.1 Trust service provider (TSP)

A party that provides trust services under eIDAS regulation (EU) and/or ZertES regulation (Switzerland).

1.3.2 Certificate authorities (CA)

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

PXL Vision AG does not operate a CA but offers identification services on behalf of CAs.

1.3.3 Registration authorities (RA)

A Registration Authority 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.

PXL Vision does not operate as RA but offers identification services on behalf of a CAs RA.

1.3.4 Subscribers

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

PXL Vision identifies the subscribers on behalf of contracted partners or CAs.

1.3.5 Relying parties

A Relying Party or contracted partner is an individual or entity that relies on a certificate.

A Relying Party or contracted partner uses a subscriber's certificate to verify the integrity of a digitally signed document and to identify the signer of the document.

1.3.6 Other participants

PXL Vision's PXL Ident web application provides online identity document validation and biometric verification services for TSPs during their CA/RA activities, i.e., enrollment, renewal, and reactivation of electronic identities for digital certificates for natural persons. PXL Vision is ISO 27001-certified and scoped to identity verification services.

A public cloud provider is a subcontractor of PXL Vision and hosts the PXL Ident servers that processes all identity document data and orchestrates any data exchanges. There is a contractual agreement between the public cloud providers and PXL Vision. The PXL Ident service is provided as a SaaS. The organizational/contractual and technical security measures provided by the cloud providers meet the relevant requirements

laid down by eIDAS, ZertES and ETSI for TSPs. It is the responsibility of PXL Vision to control and monitor this process. Consequently, security requirements in terms of certifications are set for the public cloud providers.

1.4 Policy administration

1.4.1 Organization administration
This IPSPS is administered by PXL Vision AG, Rautistrasse 33, CH-8047 Zürich

1.4.2 Contact person
For certification purposes, PXL Vision can be contacted via Certifications@PXL-Vision.com

1.4.3 Person Determining CPS Suitability for the Policy
PXL Vision's Contact Person determines the suitability of this IPSPS with the Policy.

1.4.4 IPSPS Approval Procedures
The IPSPS document and all amendments must be approved by PXL Vision Executive Management before becoming effective and being published and communicated to relevant employees and external parties.

1.5 Definitions and Acronyms

1.5.1 Definitions
- App: Application running on user's phone
- Web App: Web Application running through a web browser on the user's mobile device
- ID Document: An official and government issued identity document such as passports, driving licenses, or identity cards.
- Biometric ID Document: ID Document that includes a biometric NFC-readable chip as defined by the ICAO Doc 9303 specification
- Security features: Specific security features present on the ID Document or Passport, as holograms, lenticulars, or other formats
- User: The natural person using the identity verification services, defined as subscriber
- Document Validation: The process of extracting and verifying the information available on the identity document
- Face Verification: The process of biometrically comparing a live or captured facial image or video to a reference image to verify that they belong to the same individual
- Liveness Detection: The verification that the features being presented to the biometric application are those of a living subject, and not a copy or imitation of those features

1.5.2 Acronyms
- AI/ML: Artificial Intelligence / Machine Learning
- BSI: (German) Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
- CA: Certification Authority
- CISO: Chief Information Security Officer
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- DPA: Data Processing Agreement
- DPIA: Data protection impact assessment
- DPO: Data Protection Officer
- DSG: (Swiss) Datenschutzgesetz (Data Protection Law)
- eIDAS: EU regulation for electronic identification and trust services for electronic transactions
- ETSI: European Telecommunications Standards Institute
- GDPR: EU General Data Protection Regulation
- ICAO: International Civil Aviation Organization
- IPSPS: Identity Proofing Service Practice Statement
- ISMS: Information Security Management System
- MRZ: Machine Readable Zone
- NFC: Near Field Communication
- PII: Personally identifiable information
- PKI: Public Key Infrastructure
- QTSP: Qualified Trust Service Provider
- RA: Registration Authority
- REST API: REST (Representational State Transfer) Application Programming Interface
- SaaS: Software as a Service
- SLA: Service Level Agreement
- TLS: Transport Layer Security
- TSP: Trust Service Provider
- TSPS: Visual Inspection Zone
- VIZ: Visual Inspection Zone
- ZertES: Swiss Federal regulation under which trust service providers may use certification services with electronic signatures

1.5.3 References
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI);
  General Policy Requirements for Trust Service Providers
  v2.3.1 of May 2021
- ETSI TS 119 461: Electronic Signatures and Infrastructures (ESI);
  Policy and security requirements for trust service components providing identity proofing of trust service subjects,
  v1.1.1 of July 2021
- eIDAS: Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, amended by regulation 2024/1183 on 11 April 2024
- ICAO Doc 9303: ICAO document on passports and electronically readable fields
- TR-03116-4: Technical requirements for encryption and encrypted transmission, from German BSI
- ZertES: Swiss Federal Act of 18 March 2016 on the Electronic Signature (SR 943.03) and Ordinance of 23 November 2016 on the Electronic Signature (SR 943.032)
- ISO 30107-3: Information technology — Biometric presentation attack detection, Part 3: Testing and reporting

2 Publication and Repository Responsibilities

2.1 Repositories
PXL Vision AG publishes this IPSPS and the Data Protection Statement on its website https://www.pxl-vision.com, where they

are available 24x7. Terms of use for the identification service are accessible via the PXL Ident web application.

2.2 Time or Frequency of Publication

The IPSPS and the Terms of Use are reviewed at least once a year to stay in compliance with regulations listed in section 1.5.3. Substantial changes to the IPSPS which might affect the acceptance of the service by the subject, subscriber or relying parties, are announced at least one month prior to the change becoming effective.

2.3 Access Controls on Repositories

PXL Vision 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

This section describes the identification and authentication processes during initial registration and prolongation. It particularly focuses on the identity verification services provided by PXL Vision in order to enable the TSP to issue qualified certificates.

PXL Vision provides its services to the TSP based on a contractual agreement which includes (besides others):

- applicable terms of use including aspect of consent for steps in the procedures,
- legal duties and limitations in the interaction of both parties,
- responsibilities for interaction management
- a service level agreement and
- technical aspects of the service rendered such as the type of input and output of data

PXL Vision's identity verification steps provide an alternative to physical verification at the TSP during registration and to video-verification with a human agent. The steps taken into providing this verification are listed as below:

- Document Validation
- Face Verification
- Liveness Detection
- Manual Verification Check (mandatory for non-digital documents)

By applying all these checks in various configurations as applicable for each TSP, the identity verification process as well as proving the authenticity of the data upon which the identity verification is based, can be ensured. The TSP integrates this process performed via a web app within the registration process.

The TSP orchestrates the user registration step, after which the TSP redirects the user to the PXL Ident application, which is responsible to start the identification and authentication process of the subscriber.

The TSP communicates with the PXL infrastructure through a secured REST API, through which a request to start a new identification process is triggered.

PXL Ident Web App carries out the document validation, face verification and liveness detection as described in section 3.2. These steps - without manual checks - are fully automated and can be used 24x7. The algorithms used in this process are being continuously maintained and are secured against threats to its integrity and functions.

After completion of the process PXL Vision notifies the TSP of the results of the verification process.

3.1 Type of Names

PXL Ident recognizes and interprets names as obtained from the legal identity documents.

3.2 Authentication of Individual Identity

The authentication of the individual identity is checked in different ways. Original individual identification methods include: personal user data as extracted and validated from the MRZ/VIZ sections of the ID Document, binding the user to the ID Document by running a Face Verification and a Liveness Detection based on the picture of the face from the ID Document and the selfie video that the user needs to take.

DESCRIPTION OF METHOD: PXL Ident

The subscriber is forwarded to the PXL Vision Service by the TSP through a deep link that uniquely identifies the start of the PXL Ident Web app process. The user is then guided through a verification process that includes various checks of the full identity data.

The authentication of the individual identity is checked in three steps followed by an optional manual check, which is mandatory for non-digital documents.

- Document Validation
- Face Verification
- Liveness Detection
- Manual Check

The PXL Ident Web App follows the steps described below:

<u>Document Validation</u>

The document validation is the first step in the process and - as this - also presents the entry point from the TSP to PXL Vision.

The subscriber's identity is checked against an official, valid, government-issued photo ID document. International passports must fulfill the ICAO 9303 Standards. For this, the subscriber is asked to scan their ID Document. The PXL Ident Web App will extract and validate the information of the ID Document in real time while the user is scanning the ID document.

If supported by the mobile phone and the identity document, identity information and biometric photos are extracted from digital identity documents via an NFC read-out process.

For non-digital identity documents, the user is asked to take a recording of the security features of the document.

<u>Face Verification</u>

Next, the subscriber is asked to take a selfie video. The picture of the face captured from the ID Document is used to compare the user to the selfie video taken to verify that the person on the ID Document is the same person taking the selfie video. The assessment is done automatically by a trained AI/ML solution.

<u>Liveness Detection</u>

As a third step, a Liveness Detection is performed to ensure that the person behind the camera is a real person. It uses the same selfie video as Face Verification. The assessment is done automatically by a trained AI/ML solution.

<u>Manual Check</u>

For the cases where identity verifications cannot be completed automatically, PXL Vision performs extra verification of the identity data. This process is performed by subcontracted, fully trained and supervised resources.

The information collected during the identification process is transferred to the TSP with the results of all the checks and the results performed through the process.

All data transmission to / from communicating entities is fully encrypted in accordance with TR-03116-4.
The TSP is responsible at this stage to define if the process can be completed and accepted automatically based on the extracted data, in which case the PXL Ident Web App will redirect the user to a web page defined and controlled by the TSP, where the subscriber can continue the user journey.

3.3 Identification and Authentication for Re-key Requests

TSPs that support re-key requests may make use of the identification features described in section 3.2

3.4 Identification and Authentication for Revocation Requests

For revocation requests the TSP may make use of the identification features described in section 3.2

4 Management, operational, and physical controls

PXL Vision Executive Management has approved a general information security policy document. It is published, and communicated, as applicable, to all employees, suppliers, relying parties, assessment bodies, supervisory or other regulatory bodies affected by it.
This policy is supplemented by detailed policies and procedures for personnel involved in identity verification. 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. PXL Vision Executive management ensures that there is clear direction and visible management support for security initiatives. PXL Vision's management is responsible for maintaining the 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 IPSPS.
PXL Vision carries out regular risk assessments to identify, analyze, and evaluate risks related to its services taking into account business and technical issues. PXL Vision then selects appropriate risk treatment measures taking into account the results of the risk assessment.
The chosen risk treatment measures ensure that the level of security is commensurate with the degree of risk. The risk assessment is approved by PXL Vision Executive Management who accepts the residual risks identified in the risk assessment with this approval. PXL Vision's ISMS is ISO 27001 compliant and certified as such. The ISMS ensures that proper security controls adequate to manage the risks are taken and the information security of PXL Vision is constantly being improved upon.
Note: The requirements from section 4.1 apply to PXL Vision as well as to its external service partners relevant to providing the identification services described in section 3.2

4.1 Physical Security Controls

PXL Vision has implemented security policies which support the security requirements of the services, processes, and procedures covered by this IPSPS.
These security mechanisms are commensurate with the level of threat in the identity verification environment.

4.1.1 Site Location and Construction

All PXL Vision's operations facilities are specifically designed for computer operations.
PXL Vision operates its platform from ISO 27001-certified data centers in Switzerland and the EU. PXL Vision has effective service provider agreements in place with the data center providers ensuring appropriate security. The data centers are equipped with logical and physical controls that make PXL Vision's identity service operations inaccessible to non-trusted personnel.
In particular, backend operations related to identity verification are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. Several layers of physical security controls restrict access to the sensitive hardware and software systems used for performing operations. The systems used for identity verification services are logically separated from other systems so that only authorized employees can access them.
Relevant prevention and detection mechanisms exist to address environmental incidents, such as power loss, loss of communication, water exposure, fire and temperature changes.
In addition, PXL Vision ensures that physical access to its data centers incl. database servers, routing and switching components, and firewalls are sufficiently restricted. All IT components required for the implementation of the PXL Vision service are in specially secured locations.
PXL Vision has implemented physical access controls to reduce the risk of unauthorized persons being able to access PXL Vision's offices. Within PXL Vision's office, a clean desk policy is in place. Visitors must be registered and accompanied by authorized employees.

4.1.2 Media Storage

All sensitive media are stored digitally either in two data centers at two separate locations or - where appropriate - with public cloud service providers. The data centers are equipped with redundant servers, storage, network links and other IT components.

4.1.3 Off-site backup

PXL Vision performs regular routine backups of critical system data, audit log data, and other sensitive information (e.g. proprietary source code and other crucial software components) to a secondary site. PXL Vision is not obliged to keep identity verification data for a long period of time because all relevant identity verification data is sent to the QTSP for the purpose of issuing a qualified certificate immediately after the identity data has been collected. The QTSP is then obliged to archive these data according to the ZertES and eIDAS regulations.

4.2 Procedural Controls

4.2.1 Trusted Roles

Trusted Roles include all employees that have access to the source code or administer PXL Vision's services. A Trusted Roles concept has been implemented and the individual Trusted Roles are defined by the organisation. Personnel is kept free from conflict of interest that might prejudice the impartiality of the PXL Vision operations.

4.2.2 Number of Individuals Required per Task

PXL Vision ensures that the number of staff available for tasks is adequate to meet demand, but also adequate to ensure that all security, risk and compliance regulation requirements are met.

If a risk analysis identifies tasks as requiring dual control, then dual control is applied.

4.2.3 Identification and Authentication for Trusted Roles

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 4.3.2. The person who takes over a trusted role must agree to this before approval. Personnel have no access to the trusted functions until the necessary checks are completed.

Personnel in trusted roles are named and approved by the Executive management of PXL Vision before being permitted to access relevant systems requiring the principle of "least privilege" when accessing or when configuring access privileges.

Identification and authentication during operations for each role is based on individual privileges.

4.2.4 Roles Requiring Separation of Duties

A segregation of conflicting duties and areas of responsibility is implemented to reduce opportunities for modification and misuse to its minimum.

4.3 Personnel Security Controls

Note: The requirements stated in this chapter also apply to external service providers, outsourcing partners, and independent contractors relevant for the provisioning of PXL Vision's identity verification services.

4.3.1 Qualification, Experience, and Clearance Requirements

All employees involved in the operation of PXL Vision's services 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 information security procedures for personnel with information security responsibilities.

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

4.3.2 Background Check Procedures

PXL Vision thoroughly checks employees' qualifications for their responsibilities prior to hiring.

Training and previous employment are examined on the basis of training and work certificates.

In addition, all new employees undergo a criminal record check. This consists of presenting a certificate of conduct. The checks must be clear of records related to trustworthiness. For employees in Trusted Roles, criminal record checks are repeated every 2 years.

4.3.3 Training Requirements and Procedures

All personnel performing duties with respect to the operation of the PXL Vision systems and services receive comprehensive training including information security and data protection, which are mandatory for all PXL Vision employees. PXL Vision maintains records of Information Security and Data Privacy training performed.

4.3.4 Re-Training Frequency and Requirements

All employees are required to attend annual data protection and information security awareness training sessions. Job specific retraining is performed to the extent and frequency required to ensure that the required level of proficiency is maintained.

4.3.5 Sanctions for Unauthorized Actions

PXL Vision employees are accountable for their activities. PXL Vision employees failing to comply with this IPSPS, whether through negligence or malicious intent, are subject to internally maintained processes specifying guidance on administrative or disciplinary actions, up to and including termination of employment and legal sanctions.

4.3.6 Documentation Supplied to Personnel

All employees are provided with a contract of employment and a defined job role.

This IPSPS, applicable system operations documents, operations procedures documents, and any relevant other documents required to perform their jobs have been made available to PXL Vision employees.

4.4 Audit Logging Procedures

4.4.1 Types of Events Logged

PXL Vision 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 system access attempts. When setting up any kind of logging or monitoring activities, the security and sensitivity of the information collected is considered.

Security log entries include date/time and description/kind of entry.

The identity verification audit logs include in particular records of identification presented and identity of service requesting / providing the identity.

4.4.2 Frequency for Processing & Archiving Audit Log

PXL Vision's systems and its components are continuously monitored and can provide real-time alerts if unusual security or operational events occur and allow an immediate review by system security administrators.

Security events and audit logs are regularly reviewed including verification that the logs have not been tampered with and an

investigation of any alerts or irregularities detected in the logs. Actions taken based on security log reviews are documented.

4.4.3 Retention Period for Audit Log

Audit logs concerning the infrastructure are stored and accessible for one year, unless required otherwise by specific legislation or TSP demands.

Audit logs concerning the identification process are stored and accessible according to the applicable contracts with the customer in compliance with Swiss data protection regulation and GDPR.

4.4.4 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. Access to audit logs is restricted to authorized personnel.

4.4.5 Audit Log Backup Procedures

Audit logs are stored within the data centers which provide sufficient redundancy and geographically distinct locations.

4.4.6 Audit Collection System (Internal vs. External)

Audit logs are generated and recorded automatically at the network and operating system level.

4.4.7 Vulnerability Assessments and penetration tests

PXL Vision's systems are assessed via internal and external vulnerability scans and penetration tests. Automated vulnerability scans are carried out on public and private IP addresses with every major release of PXL Vision's software, and at least once every three months. The scans are set up, maintained, reviewed and documented by PXL Vision employees with the skills and proficiency to do so.

Penetration tests are carried out by external contractors regularly, performed at least once per year or after significant modifications. The contractors are chosen with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable assessment.

Any critical vulnerability not previously addressed by PXL Vision is addressed within a period of 48 hours after its discovery.

4.5 Records Archival

4.5.1 Types of Records Archived

At a minimum, PXL Vision records the following data for archival:

- this IPSPS
- contractual obligations
- system and equipment configuration
- modifications and updates to systems or configurations
- audit logs mentioned in section 4.4
- documentation required by compliance auditors.

4.5.2 Retention Period for Archive

All records are archived in accordance with legal or regulatory requirements.

Long term archival of evidence collected during identifications and supporting information, i.e., identification data according to the requirements of eIDAS and ZertES, is the responsibility of the QTSP. In any case, in accordance with data protection regulation all person-related data is deleted from PXL Vision's systems after the retention period has expired and in accordance with customer contracts.

4.5.3 Protection of Archive

PXL Vision protects the archive so that only authorized persons in trusted roles are able to 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 above.

PXL Vision performs regular database backups according to the criticality of the data.

4.5.4 Procedures to Obtain and Verify Archive Information

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

4.6 Compromise and Disaster Recovery

Information security incidents, such as service unavailability, integrity breaks, or loss of confidentiality, are managed according to legislation, SLAs, and internal procedures, with regular internal and external audits. PXL Vision employs incident response procedures to minimize damage, and has documented continuity plans to ensure business recovery and communication during incidents. These recovery measures, along with regular security monitoring and risk assessments, are periodically tested and updated.

4.6.1 Incident and Compromise Handling Procedures

Incidents and compromises are handled according to PXL Vision's incident response procedure and by trusted role personnel. Regular audits are conducted to monitor the effectiveness and appropriateness of the process and provide insights for potential improvements.

The incident response procedure includes steps to notify the appropriate parties, customers, auditors and authorities in line with the applicable rules of any breach of security or loss of integrity with impact on the services provided and on the personal data maintained therein within 24 hours of the breach being identified.

Where the breach of security or loss of integrity is verified to affect natural or legal persons, PXL Vision will notify the appropriate parties without undue delay. TSPs will in turn inform the subscribers.

4.6.2 Recovering Procedures if Computing Resources, Software, and/or Data are Corrupted

In case of corruption of computer resources, software and data, PXL Vision falls back to its incident response procedure.

4.6.3 Business Continuity Capabilities after a Disaster

PXL Vision maintains an emergency manual and conducts regular business continuity tests to ensure functionality of processes in case of a disaster.

4.7 Termination of Identity Proofing Service

PXL Vision 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 relevant parties to be informed, the termination plan addresses supervisory bodies, PXL Vision customers – in particular TSPs – and other partners including subcontractors and the successor operator(s).
The standard contractual agreement with the TSP provides for PXL Vision to transfer all relevant data directly as part of the identification process and for the TSP to ensure the required servicing and archiving obligations are met. Consequently, a transfer of these obligations as part of the termination is not needed. Other applicable obligations may be taken over by a successor operator as defined in the termination plan.
Termination of services and any implied costs for PXL Vision that are attached to this process, are stipulated in the individual agreement with the TSP.

5 Technical Security Controls

5.1 Specific Computer Security Technical Requirements

PXL Vision's systems are designed with security by design principles, incorporating cryptographic methods, infrastructure, and software protections to prevent unauthorized access. The identity verification system is secured with controls such as multi-factor authentication, encrypted connections, network zoning, and risk-based monitoring. Information security policies define measurable KPIs and cover topics like secure software development, access control, and infrastructure integrity. Changes to software follow strict change management procedures, including isolated testing and 4-eyes approval. Security measures, including multi-factor authentication and bi-annual review of access controls, ensure only authorized personnel have access to critical systems.
PXL Vision's IT Ops and Admin policy sets security requirements of PXL Vision's deployments and the continuous operation of its services.
The security processes comply with the specific requirements in ETSI EN 319 401 and ISO 27001. PXL Vision's ISMS is certified against these standards by independent and accredited auditors.

5.2 Life Cycle Technical Controls

PXL Vision's software development process follows best practices to minimize bugs and vulnerabilities, using version control, peer reviews, static code analysis, and automated testing. Code changes undergo several approval steps before release, including testing by TSPs when required. Larger features are subject to penetration tests, and responsibility for code is always assigned to ensure accountability. Development guidelines include dependency assessments, source code quality checks, and strict versioning and release procedures. All operational systems are regularly monitored, with automated alerts to ensure their integrity and proper functioning.

5.3 Life Cycle Security Controls

PXL Vision reviews its information security policies, assets, and practices annually or after significant changes to ensure their effectiveness. System configurations are continuously checked for compliance with security policies, and the CISO reviews security-impacting changes. Security patches are applied promptly unless they introduce greater risks, with reasons for delays documented. PXL Vision maintains an overview of information assets classified by security level, with designated personnel responsible for their security.
All user accounts and all firewall rules are reviewed and re-validated twice per year.

5.4 Network security controls

PXL Vision separates its network into zones with varying security measures based on the criticality of services and data, managed by a dedicated team. Firewall rules are applied and regularly reviewed, with unnecessary services deactivated by default. Strong authentication, including digital certificates and multi-factor authentication, is required for internal and external communications, as well as administrator access. Data centers at separate sites ensure redundancy, and all communication between sites and with users is encrypted and authenticated using TLS. PXL Vision manages the security of its Kubernetes-based infrastructure, while external data center providers handle physical and network infrastructure security. PXL Vision requires providers to maintain ISO 27001 certification or equivalent, and TSPs connected to the platform follow their own security measures as outlined in their Trust Service Practice Statements.

5.5 Time-Stamping

Audit logs and transactions are time-stamped based on a reference clock service. This reference clock is synchronized via NTP with reliable sources.

6 Compliance Audits and Other Assessments

6.1 Frequency and Circumstances of Assessment

PXL Vision is subject to regular external audits, including audits pursuant to ETSI EN 319 401 and ETSI TS 119 461. The results of these compliance audits are documented and archived. According to eIDAS, compliance audits must be performed at least every 24 months and surveillance audits within 12 months after each full audit. The same is applied to maintain ZertES compliance.

6.2 Identity/Qualifications of Assessor

The conformity assessment is performed by an appropriately accredited conformity assessment body.

6.3 Assessor's Relationship to Assessed Entity

External auditors are independent and have no business interests in PXL Vision. No external auditor has any business affiliation with PXL Vision.

6.4 Topics Covered by Assessment

The purpose of a compliance audit is to verify that PXL Vision's service complies with the statements of this IPSPS, with the eIDAS and ZertES regulations, and with the requirements specified in the audit standard under consideration. All applicable aspects of this IPSPS and all the standards mentioned in this section 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.

6.5 Actions Taken as a Result of Deficiency

If deviations are identified during the compliance audit as defined in this section, corrective actions are drafted to correct the deviations. The corrective actions are agreed upon with the external auditor.

6.6 Self-Audits
At least once a year, PXL Vision carries out regular internal audits to continuously assess compliance with the laws, regulations, internal policies and requirements mentioned in this document.

7 Other Business and Legal Matters

7.1 Fees
Fees for the identity verification services are subject to contractual agreements between PXL Vision and the TSP and/or the Customer. Specific commercial agreements may vary per TSP and/or Customer.

Usage of PXL Vision's Service is free of charge for the subscribers.

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

7.2 Financial Responsibility - Insurance Coverage
PXL Vision undergoes regular financial assessments to verify that it has the financial stability and resources required to operate in conformity with this IPSPS and the requirements of eIDAS and ZertES. PXL Vision maintains a professional liability insurance coverage.

7.3 Confidentiality of Business Information

7.3.1 Scope of Confidential Information
In the framework of the established and ISO 27001-certified ISMS, the level of confidentiality of information is determined. Three levels of confidentiality are distinguished: public, internal, and confidential. Confidential information includes in particular any information provided by users for the purpose of identity verification.

7.3.2 Information Not Within the Scope of Confidential Information
Documents and other information classified within the ISMS classification scheme as public are not considered confidential information.

7.3.3 Responsibility to Protect Confidential Information
PXL Vision, its employees and all other participants described in this IPSPS have a responsibility to protect confidential information in their possession in accordance with this IPSPS, in accordance with contractual agreements, and in accordance with Swiss law, EU law and other applicable data protection regulations.

7.4 Privacy of personal information
Within the scope of this IPSPS, PXL Vision and the TSP act as data controller for their respective services. Users are informed in the Privacy Policy that data will be transferred acoording to the requirements of the service provision and interaction between PXL Vision and the TSP.

PXL Vision has appointed a DPO, whose task is to ensure that the organization processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules.

PXL Vision has performed a DPIA for its identity verification service, which provides an overview of the personal data being processed, identifies the risks associated with the processing of the data and describes the technical and organizational control measures implemented to mitigate the risks.

Optionally, PXL Vision may act as a commissioned data processor of personal data for the customer. In these cases, PXL Vision is bound by a DPA in conformity with Swiss DSG and GDPR. The Customer then acts as the data controller and is responsible towards the subscriber to ensure data protection according to the law and as outlined in its privacy statements available from the Customer.

7.4.1 Information Treated as Private
Applicable data privacy law defines which information must be treated as private. Further information to be treated as private can be contractually agreed upon.

7.4.2 Information not Deemed Private
Information included in the certificates that are issued by a CA based on identity verifications performed by PXL Vision is not considered to be private.

7.4.3 Responsibility to Protect Private Information
All employees of PXL Vision receiving such information are obliged to protect it from compromise and disclosure to third parties and must adhere to applicable privacy laws.

Every employee at PXL Vision, as well as any commissioned agents working for a contractor bound to PXL Vision by a DPA, goes through regular privacy training during his employment and takes an online test on data protection.

PXL Vision ensures protection of PII by implementing security controls as described in chapter 4 and chapter 5 of this IPSPS.

7.4.5 Notice and Consent to Use Private Information
Unless otherwise stated in this IPSPS, PXL Vision will not use PII without the owner's consent.

7.4.6 Disclosure Pursuant to Judicial or Administrative Process
PXL Vision will only fulfill the requirements to supply data for forensic purposes as required by law enforcement and for the judicial process, per the legal administrative procedures.

7.4.7 Other Information Disclosure Circumstances
There are no other information disclosure circumstances.

7.5 Intellectual Property Rights
Any intellectual property rights associated with products and services supplied by PXL Vision, and associated materials, remain the property of PXL Vision, the licensor or supplier. All information regarding conditions pertaining to intellectual property rights can be found in the associated terms and conditions and any contractual agreements.

PXL Vision services include the capturing of images or videos by the subscribers with their mobile device. Depending on the local legislative situation, it may be necessary for PXL Vision to have the moral rights, copyrights or rights on one´s own picture transferred or granted as usage rights from the subscriber as the legal creator and person depicted. PXL Vision informs the subscriber about this requirement in their Terms of Use.

7.6 Representations and Warranties
PXL Vision can be party to mutual agreements and obligations between the TSP, the customer, the subscriber and other

participants. This IPSPS forms an integral part of these agreements.
PXL Vision will supply true and adequate information in the application for the services.
As an ISPS, PXL Vision warrants that each subscriber has been identified and authenticated properly prior to proceeding to the TSP for execution of the further steps related to the issuing of corresponding certificates. PXL Vision does not warrant the identification result being provided to the TSP within real time, since manual checks may be required that only operate during applicable working hours.
PXL Vision does not warrant a successful identification, if prerequisites to be met by the subscriber (see section 7.6.3) are not fulfilled. PXL Vision may refuse to provide the service if the subscriber has intentionally presented false, incorrect or incomplete information in the application for the service.
PXL Vision also doesn't warrant the timely or executable transfer of information to the TSP in case of network outages beyond PXL´s control.
It is emphasized that it is up to the TSP to finally issue the requested certificates or QES. The customer relationship between the TSP and the user is beyond PXL Vision´s control. PXL Vision only assures the correct identification as set out in this IPSPS.
PXL Vision strives to optimize the experience of its services by the subscriber in terms of usability, intuitively, and accessibility as much as possible and does its best to provide its services in a way suitable for subscribers with disabilities but does not warrant that their services are fully barrier-free for all kinds of disabilities.

7.6.1 CA Representations and Warranties
Does not apply

7.6.2 RA Representations and Warranties
Towards the specific RA part of the TSP, PXL Vision warrants to:
provide its services consistent with the requirements and the procedures defined in the contract between PXL Vision and RA, in this IPSPS and service-based Policies and Practice statements - in particular to forward complete, accurate, and verified data about subjects for further processing;
provide its employees and subcontractors with necessary training for supply of high-quality service;
without undue delay after having become aware of it, notify RA of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

7.6.3 Subscriber Representations and Warranties
It is the subscriber´s obligation to provide truthful and correct information, to use compatible devices that are securely set up, and to ensure a working environment that allows the proper capture of the information and imagery required for the identification process.

7.7 Disclaimers of Warranties
No limitations of warranties apply other than those mentioned in section 7.6

7.8 Limitations of Liability
PXL Vision is liable towards the TSP and/or the customer for the correctness of the results of the identification process according to the contractual provisions with the TSP and/or the customer. Except for cases of intent, gross negligence and damages to life, limb and health or except such is otherwise legally required PXL Vision has no liability towards the subscribers.

7.9 Term and Termination

7.9.1 Term
The IPSPS is effective upon publication on PXL Vision's website. Amendments to this IPSPS become effective upon publication.

7.9.2 Termination
By publishing a new version of the IPSPS, the previous version of the IPSPS is automatically rendered obsolete.

7.9.3 Effect of Termination and Survival
Despite the fact that this IPSPS may eventually no longer be in effect, the following obligations and limitations of this IPSPS shall survive

- section 7.2 (Financial Responsibility)
- section 7.3 (Confidentiality of Business Information), and
- section 7.6 (Representations and Warranties).

7.10 Individual notices and communications with participants
PXL Vision does not provide notifications to subscribers; this will always be done by the TSP.

7.11 Procedure for Amendment
Amendments to this IPSPS may be made by PXL Vision's Executive Management. Amendments shall either be in the form of a document containing an amended form of the IPSPS or an update. Amended versions or updates shall be published in the repository.

7.12 Dispute Resolution Provisions
PXL Vision only provides identity verification services in order to support the registration authorities of the CAs that issue the certificates.
For disputes with end-users and relying parties the dispute resolution procedures of the issuing TSPs apply.

7.13 Governing Law
PXL Vision, situated in Switzerland, is subject to national Swiss Laws for the provision of services and products.

7.14 Compliance with Applicable Law
PXL Vision's solution provides identity verification services to the TSP as defined in EU eIDAS regulation and Swiss ZertES regulation. This requires PXL Vision to be compliant to the applicable requirements of the following standards, requirements, and regulations:

- ISO 27001 Information Security Management System
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ETSI TS 119 461 Policy and security requirements for trust service components providing identity proofing of trust service subjects
- eIDAS Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- ZertES Swiss Federal Law SR 943.03 on certification

services in the area of the electronic signature

- GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

7.15 Miscellaneous provisions

7.15.1 Severability

If parts of any of the provisions in this IPSPS are incorrect or invalid, this shall not affect the validity of the remaining provisions until the IPSPS is updated. The process for updating this IPSPS is described in section 7.11

7.15.2 Force Majeure

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