Identity Proofing Service Practice Statement

Cleverbase

Version 1.2.0

15-06-2026

This is the official version of the Cleverbase Identity Proofing Service Practice Statement.

Hierarchy of documentation

This document is written with due care. However, in case of discrepancies between other documents, the following hierarchy exists:

- The privacy statement
- The certification practice statement
- The identity proofing service practice statement
- PKI disclosure statement
- The terms & conditions in Dutch
- The terms & conditions in English
- The product conditions in Dutch
- The product conditions in English
- Other public outings by Cleverbase

Table of Contents

1 Introduction

1.1 Overview

Cleverbase is a qualified trust service provider, who also acts as Identity Proofing Service Provider (IPSP) under the international standard ETSI TS 119 461 v2.1.1. Cleverbase's identity proofing service is limited to the identity proofing for natural persons. Cleverbase's identity proofing service uses a mobile application that Cleverbase develops and provides itself.

Cleverbase supports different identity proofing use cases as identified in ETSI TS 119 461 and under eIDAS article 24.1a . This document is the Identity Proofing Service Practice Statement for all supported use cases. All supported use cases are compliant with Level of Identity Proofing Extended, or as identified by eIDAS article 24.1a (910/2014 and 2024/1183).

In all supported identity proofing processes, Cleverbase undertakes the following steps: - Verifies agreement with the Product Conditions - Authenticates the presented identity document - Matches the presented identity document to the individual subscriber - Verifies live attendence ('liveness')

Cleverbase's Identity Proofing Service supports two identity proofing contexts: - It fulfils the role of Registration Authority (RA) for Cleverbase's Certificate Authority (CA). The final result of the Identity Proofing service is a certificate signing request for Cleverbase's CA. The certificate(s) issued can be used for the purposes described in the Certification Practice Statement. Cleverbase's practices as a CA are described in its Certification Practice Statement. - It collects and verifies personal data so that users can share their data with the highest level of assurance as recognised by the EU, for example for identification in AML-processes. This trust service is Wwft-compliant.

1.2 Document Name and Identification

This document is Cleverbase's Identity Proofing Service Practice Statement (IPSPS). It describes the practices the IPSP employs with regards to the Identity Proofing of natural persons. This IPSPS is based on Regulation (EU) 910/2014 (eIDAS)(32014R0910 - EN - EUR-Lex), and ETSI TS 119 461 (available at https://www.etsi.org/standards). Any requirements on Identity Proofing for natural persons laid down by the PKIoverheid Programme of Requirements (PoR) (available at PKIoverheid Programme of Requirements) or ETSI standards EN 319 411-1 and EN 319 411-2 (both available at https://www.etsi.org/standards) are also in scope of this document. Its structure is modelled after RFC 3647 insofar as appropriate.

1.3 Participants

1.3.1 Certification Authorities

Cleverbase is the Certification Authority (CA) who uses the outcome of the Identity Proofing Service as described in this document in order to complete certificate applications. Cleverbase's practices as a CA are described in its Certification Practice Statement (CPS).

1.3.2 Registration Authorities

Cleverbase is the registration authority (RA) for the certificates it issues as certificate authority (CA). Its practices as Registration Authority are described in this IPSPS. The final result of the Identity Proofing process is a certificate generation request to Cleverbase's CA.

The RA can either mean the organisation Cleverbase, or the logical technical component that contains all functionality required to execute identity proofing. The IPSP is a synonym for the RA in the oranisational sense.

1.3.3 Subscribers

Within the scope of this document, subscribers are natural persons who have accepted the Product Conditions.

1.3.4 Relying Parties

A relying party may be any natural or legal person who relies on the used trust service by a natural person that has been identified using Cleverbase's Identity Proofing.

1.3.5 Other Participants

Other participants under this IPSPS include regulatory and supervisory bodies, suppliers of hardware, suppliers of software and equipment, as well as other supporting parties. In particular, these include the Policy Authority (PA) is PKIoverheid, who set the standards within which Cleverbase can execute its Identity Proofing. Cleverbase ensures that all suppliers act in accordance with relevant regulations. Cleverbase has appropriate controls in place to maintain adherence to said practices and regulations.

1.4 Usage

Identity Proofing shall be used in accordance with the applicable Product Conditions.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This document is published and maintained by Cleverbase ID B.V. It is revised at least once a year.

Minor updates increase the version number by 0.1; major revisions lead to a new version. Minor updates can be published without prior announcements. Revisions that might affect a user's acceptance of the Product Conditions will be announced on Cleverbase's website before coming into force.

1.5.2 Contact person

In case of questions about this document or otherwise, Cleverbase can be contacted on 070 820 96 80 or klantenservice@cleverbase.com.

1.5.3 Person Determining IPSPS Suitability for the Policy

The PA determines the suitability of this IPSPS in respect of their CP.

1.5.4 IPSPS Approval Procedures

The TSP's management has the final authority for approval of the IPSPS. In case of minor changes, they have delegated approval authority.

1.6 Definitions and Acronyms

Abbreviation	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
eIDAS	European regulations 910/2014 and 2024/1183
IPSPS	Identity Proofing Service Practice Statement
IPSP	Identity Proofing Service Provider
LoIP	Level of Identity Proofing
PA	Policy Authority
RA	Registration Authority

2 Publication and Repository Responsibilities

2.1 Repositories

Cleverbase has an electronic repository which holds its documentation dissemination.

2.2 Publication of Certification Information

At a minimum, the following information is accessible via the documentation dissemination service via cleverbase.com/en/legal: - this Identity Proofing Service Practice Statement; - the product conditions; - the privacy statement.

This document is available in English and aims to satisfy the requirements laid down by ETSI TS 119 461. Its current version is available 24 hours a day and 7 days a week. In case of disruptions, the maximum recovery time is 24 hours.

2.3 Time or Frequency of Publication

A new version of this document is published after a revision and at least annually. The Product conditions are published after a revision.

2.3.1 Accessibility of repositories

The current version of this document is available at https://pki.cleverbase.com/IPSPS.pdf. Earlier versions of this document, and other documents held by the documentation dissemination service, are available at https://cleverbase.com/en/legal.

2.4 Access controls on repositories

This document is secured against unauthorised modifications. Only Cleverbase is authorised to modify this document.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Data

During the identity proofing process, the following personal data is collected an verified to ensure the unique binding of the applicant.

Data	Description
Given name	Given names as listed on the subscriber's identity document
Surname	Surnames as listed on the subscriber's identity document (married name not included)
Common name	Combination of given name and surname
Prefix	Surname's prefix as listed on the subscriber's identity document, if applicable
Nationality	Nationality as listed on the subscriber's identity document
Date of birth	Date of birth as listed on the subscriber's identity document
Place of birth	Place of birth as listed on the subscriber's identity document
Register membership number	[OPTIONAL: Profession certificates for `Registeraccountant` and `Accountant-Administratieconsulent`] Register membership number issued by the Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA)

During the identity proofing process, the following attributes of the authoritative evidence are collected:

Attribute	Description
Document number	Document number as listed on the subscriber's identity document
Expiry date	Expiry date as listed on the subscriber's identity document
Date of Issuance	Date of issuance as listed on the subscriber's identity document
Issuer	The issuing country of the identity document.
Authority	Formal authority having issued the subscriber's identity document

This data is collected for all supported use cases.

3.1.2 Need for Data to be Meaningful

All personal data has a meaningful and verifiable relation to the subscriber, as derived from an authoritative source.

3.1.3 Anonymity or Pseudonymity of Subscribers

Pseudonyms or anonymous names are not accepted. In exceptional cases, it is possible that an identity document lists a place of birth or a name of birth as Unknown. In this case, Cleverbase allows this data to remain unknown. It is up to the relying party to decide whether or not this is acceptable for them.

3.1.4 Rules for Interpreting Various Data Forms

All data collected and verified is copied from the identification document exactly, with the following exceptions:

- If the common name exceeds the character limit of 64 characters, one or more first names will be replaced with initials, starting with the last full name, and stopping when the common name no longer exceeds the character limit.
- If first names are abbreviated to initials in the common name, the same is done for the given name.
- If the identification document provides data both in a Latin and a non-Latin script, the Latin version is used.
- Capital and lowercase letters are considered identical.
- If data contains special characters that are not supported by the MES-1 character set, the character will be transliterated according to a transliteration list.
  - If the character is not contained in the transliteration list, it will be transliterated to the closest available character in the 26-character Latin alphabet.
- The nationality is encoded in the two-letter ISO3166-1 notation.

3.2 Initial Identity Validation

Cleverbase uses their dedicated mobile application to identify natural persons and verify their identities for the issuance of qualified certificates. Cleverbase supports several use cases for identification:

Remote unattended hybrid (approval by supervisor RDI pending)	Remote attended hybrid	Remote attended manual
Identification is done using biometric binding.	Identification is done by a registration officer through a live video call.	Identification is done by a registration officer through a live video call.
Document authentication is done through NFC-tooling.	Document authentication is done through NFC-tooling.	Document authentication is done by a registration officer through a live video call.

The measures taken in all use cases are assessed and protect agains 'high attack potential' in accordance with EU SCSA ENISA "Methodology for Sectoral Cybersecurity Assessments, EU Cybersecurity Certification Framework"

3.2.1 Authentication of Individual Identity

In the identity proofing process, the below steps are completed at a minimum to identify the subscriber and verify the subscriber's identity.

Remote attended manual	Remote attended hybrid	Remote unattended hybrid
	ETSI TS 119 461 v2.1.1 (2025-02) Use case 9.2.2.2	ETSI TS 119 461 v2.1.1 (2025-02) Use case 9.2.3.2
User accepts Product Conditions	User accepts Product Conditions	User accepts Product Conditions

Remote attended manual	Remote attended hybrid	Remote unattended hybrid
User submits a face photo	User submits a face photo	User submits a face photo
User submits a photo of a valid and supported identity document; data is extracted from the MRZ	User submits a photo of a valid and supported identity document; data is extracted from the MRZ and RFID-chip	User submits a photo of a valid and supported identity document; data is extracted from the MRZ and RFID-chip
	Identity document is authenticated server-side	Identity document is authenticated server-side
	User undergoes biometric scan, which records a video sequence, matches the user to the submitted photos, and verifies liveness	User undergoes biometric scan, which records a video sequence, matches the user to the submitted photos, and verifies liveness
Registration officer verifies data quality	Registration officer verifies data quality	Registration officer verifies data quality
Registration officer updates data if necessary	Registration officer updates data if necessary	Registration officer updates data if necessary
Registration officer matches user to the submitted photos	Registration officer matches user to the submitted photos	Registration officer matches user to the submitted photos
Registration officer checks whether user already has a profile	Registration officer checks whether user already has a profile	Registration officer checks whether user already has a profile
Registration officer initiates a video call	Registration officer initiates a video call	
Registration officer verifies caller's identity against the submitted photos	Registration officer verifies caller's identity against the submitted photos	
Registration officer authenticates identity document		
Registration officer verifies user's liveness	Registration officer verifies user's liveness	
Registration officer terminates video call	Registration officer terminates video call	
Registration officer verifies Register membership number of accountants at the NBA *	Registration officer verifies Register membership number of accountants at the NBA *	Registration officer verifies Register membership number of accountants at the NBA *
Registration officer approves identity validation	Registration officer approves identity validation	Registration officer approves identity validation
User reconfirms PIN	User reconfirms PIN	User reconfirms PIN
A second registration officer reviews the identity validation	A decision is made whether a second registration officer reviews the identity validation, riks based	A decision is made whether a second registration officer reviews the identity validation, riks based
The second registration officer approves certificate issuance	The second registration officer approves issuance if applicable	The registration officer approves issuance if applicable

The user has the option to object to the biometric scan. Objecting the biometric scan is possible, yet it implies that the user continues in the Remote Attended Hybrid use case with a second registration officer reviewing the identity validation.

If any of the steps are not completed with positive result, the steps either have to be retaken or the process will be terminated.

* This step only applies to identity proofing steps in case of Profession Certificate requests for accountants and accountant-Administratieconsulents. Response by the NBA can take up to 14 days.

3.2.2 Supported Identity Documents

The identity proofing service accepts passports or national identity cards that comply with the International Civil Aviation Organisation standard (ICAO 9303) regarding the use NFC and Visual Inspection Zones. Driver's licences or other identification documents are explicitly excluded. The list of countries whose identity documents are currently supported is maintained on the Cleverbase website. Cleverbase reserves the rights to make risk-based exceptions for supporting specific identity document models.

For all supported use cases, the identity document is the authoritative evidence for the data that is collected.

3.2.3 Availability of Services

Cleverbase's identity proofing service is available within its opening hours. These opening hours can be found on the website https://cleverbase.com.

In case of a disruption of the identity proofing service, Cleverbase aims to resume operationality within 8 hours.

Cleverbase's mobile app for identity proofing is available in Dutch and English. Video operators are available in Dutch and in English.

4 Identity Proofing Subscription

4.1 Identity Proofing Application

4.1.1 Who Can Apply for Identity Proofing

Any natural person at least 18 years of age and in possession of a valid identity document that is supported by Cleverbase can apply for identity proofing. The person has to apply for identity proofing themselves, this cannot be done by a representative.

4.1.2 Enrolment Process and Responsibilities

The Subscriber is responsible for adhering to the requirements laid down in the Product Conditions and Identity Proofing Service Practice Statement. Identity proofing is subject to the Product Conditions and the Identity Proofing Service Practice Statement that were actual and accepted at the beginning of the identity proofing process. In the exceptional case that a new IPSPS or new Product Conditions are published within the timespan of the Subscriber accepting them and completing the process, the accepted versions remain the applicable ones.

The Subscriber is responsible for providing Cleverbase with correct and actual information at all times. If there are indications that any information that is provided is not correct or actual, Cleverbase is responsible for terminating the identity proofing process with negative result.

4.2.1 Application Processing

4.2.1 Performing Identification and Authentication Functions

Identification and authentication are done as described in section 3.2 Initial Identity Validation. The RA does not reuse previously submitted evidence.

4.2.2 Approval or Rejection of Identity Proofing

The IPSP will approve or reject identity proofing based on the outcome of the steps described in section 3.2 Initial Identity Validation.

The IPSP aims to incorrectly reject no more than 2% of genuine identity proofing attempts of proper quality, i.e. a False Rejection Rate (FRR) of 2% over the whole process; the IPSP aims to accept no more than 0.5% attempts that were of insufficient quality or were not genuine, i.e. a False Acceptance Rate (FAR) of 0.5% for the overall process. This is in line with industry best practice. The IPSP will regularly evaluate whether industry best practice has improved.

The biometric solution that Cleverbase uses is tested in an independent lab in order to ensure its effectiveness in recognising Presentation Attack Instruments (PAIs). Cleverbase requires the used solution to have an APCER of at most 0.5% and a BPCER of at most 1.0%.

4.2.3 Time to Process Identity Proofing

The usual time to process identity proofing is within 24 hours. At several points in the identity proofing process, action is required from the Subscriber. For identity proofing to be completed within 24 hours, swift action is required from the Subscriber.

If the Subscriber abandons the process before the confirmation of the collected data, the Identity Proofing expires after 48 hours of inactivity.

Identity proofing for Accountants can take up to 14 days due to the verification process for claims at the NBA. After receiving verification response from the NBA subjects shall be informed about the resulting actions (e.g. Certificate issuance).

4.3 Identity Proofing Completion

4.3.1 RA Actions During Completion

The process is completed by a registration officer, see section 3.2 Initial Identity Validation. It is not technically possible for one person to submit and complete the same application.

4.3.2 Notification to Subscriber by the RA of Completion of Identity Proofing

The Subscriber receives an email once identity proofing is completed.

4.4 Identity Proofing Renewal

The process for renewing identity proofing is identical to the process described in section 3.2 Initial Identity Validation.

4.5 Identity Proofing Modification

Identity Proofing results cannot be modified. If the data collected during Identity Proofing is no longer actual, the Subscriber is obliged to have their profile deactivated. The Subscriber can apply for reactivation of their profile with new data if desired.

4.6 End of Subscription

During identity proofing, a user can terminate their identity proofing application at any moment of their choosing. After a successful identity proofing application, subscription can be ended by Certificate Revocation. Please refer to Cleverbase's Certification Practice Statement.

5 Facility, Management and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Cleverbase is located in The Hague, The Netherlands.

5.1.2 Physical Access

Cleverbase operates in a shared office building, in which they have their own dedicated office space. Cleverbase keeps the key cards with which their dedicated office space can be entered.

5.2 Procedural Controls

5.2.1 Trusted Roles

The IPSP's staff members are assigned various trusted roles with corresponding responsibilities. Their authorisations correspond to their roles. Roles include: 1. Security officers: overseeing that established security guidelines are implemented and observed. 2. System auditors: having a supervising role and assessing independently how business processes are arranged/organised and to what extent reliability requirements are met. 3. System administrators: administering the IPSP systems, including installation, configuration, and maintenance of the systems. 4. System operators: responsible for the daily management of the IPSP-systems. 5. Registration officers: responsible for executing the identity proofing process 6. Main Registration Officers: assists regular registration officers in case of questions or doubts

5.2.2 Number of Persons Required per Task

Cleverbase's critical processes are under dual control. What processes these are is defined in internal policy documents. When deciding the number of persons required for a task, the IPSP takes into account, at a minimum:

- Potential impact of genuine mistakes
- Yield of executing a task fraudulenty on purpose

5.2.3 Roles Requiring Separation of Duties

Cleverbase internally maintains a role separation matrix in which it clarifies what duties can and cannot be combined. The separation of duties considers at a minimum:

- Risk of commercial pressure compromising decisions for security personnel
- Separation of administration, operation, and evaluation tasks

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All organisation members undergo background screening before entering into service with Cleverbase. Clearance is, at a maximum, granted up to the level required for an organisation member to fulfil their role.

5.3.2 Background Check Procedures

At a minimum, a Certificate of Conduct, resume, and identity document are verified. Screening intensity is adjusted to the confidentiality level of an organisation member's intended role.

All organisation members sign a nondisclosure agreement as part of their employment contract.

5.3.3 Training Requirements

Organisation members are trained on relevant procedures.

5.3.4 Retraining Frequency and Requirements

All organisation members receive general and topic specific retraining at internally recorded frequencies.

5.3.5 Job Rotation Frequency and Sequence

Job rotation is not required.

5.3.6 Sanctions for Unauthorised Actions

Unpermitted or unethical actions by organisation members may entail disciplinary measures.

5.3.7 Independent Contractor Requirements

Contractors are considered organisation members and thus adhere to all listed requirements.

5.3.8 Documentation Supplied to Personnel

Cleverbase provides its organisation members with the documentation required to execute their work.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

In the Identity Proofing Service, the following events are recorded in the audit log:

- Start of Identity Proofing process
- Acceptance of Product Conditions

- Submitting of evidence
- Verification of evidence by Cleverbase
- Initial acceptance or rejection of Identity Proofing
- Verification of data by Subscriber
- Review outcome of Identity Proofing process

The following data are included in the audit log, if applicable:

- Date and time
- User ID
- Name and description of the event

For events that are not specific to the Identity Proofing Service, audit logging is done as described in Cleverbase's CPS.

5.4.2 Frequency of Processing Log

Audit logs are processed upon the happening of any of the events mentioned in section 5.4.1.

5.4.3 Retention Period for Audit Log

Audit logs are stored and accessible for ten years.

5.4.4 Protection of Audit Log

The Audit Log is protected from modification. The Audit Log is subject to back-up procedures to ensure its continued availability. The Audit Log is protected against unauthorised consultation.

5.4.5 Audit Log Backup Procedures

Audit Log backups are encrypted and stored at more than one location.

5.4.6 Audit Collection System (Internal vs. External)

Audit logs are collected internally. Upon unavailability of the audit log, any process that requires audit logging is interrupted until the audit log is available again.

5.4.7 Notification to Event-causing Subject

Audit logging is a standard process and event-causing subjects are, as a rule, not informed they are causing an event.

5.4.8 Vulnerability Assessments

The audit log and components supporting the audit log are in scope of Cleverbase's vulnerability management policy and procedures.

5.5 Records Archival

5.5.1 Types of Records Archived

The following types of records are archived:

- Records that are relevant for the compliance audit
- Records that have to be archived by law
- Records that are relevant for binding subscribers to their profiles

Please refer to the Privacy Statement for detailed information about what personal data is archived.

5.5.2 Retention Period for Archive

Archives are retained for ten years. For information about how the IPSP disposes of archives after their retention period, please refer to Cleverbase's Privacy Statement.

5.5.3 Protection of Archive

Archives are secured against modification, deletion, storage deterioration, and unauthorised access.

5.5.4 Archive Backup Procedures

The entire archive is backed up off-site.

5.5.5 Requirements for Time-stamping of Records

Records are provided with a timestamp using a clock that is synchronised at least once a day.

5.6 Compromise and Disaster Recovery

The IPSP has processes in place for handling calamities. A calamity is a situation in which the integrity of certificates is impaired by a cause within the IPSP's sphere of influence. Such situations include, among others:

- Large-scale compromise of integrity or confidentiality of user data
- Service unavailability considerably exceeds service level agreements

5.6.1 Incident and Compromise Handling Procedures

The IPSP has processes in place for handling (security) incidents.

5.6.2 Business Continuity Capabilities After a Disaster

The IPSP has a Business Continuity Plan in place describing the measures to prevent a disruptive incident or disaster from occurring. If such an event were to take place, the measures and services to return to the default situation are described.

5.7 RA Termination

If the IPSP terminates its RA, it will try to transfer the RA service provision to another IPSP in order to minimise inconveniences for Subscribers and other stakeholders. The IPSP has a termination plan and allocated funds in place to support termination in the least impactfull way.

6 Compliance Audit and Other Assessments

6.1 Frequency or Circumstance of Assessment

Cleverbase is an Identity Proofing Service Provider as meant in eIDAS. As such, it is subject to supervision by the Rijksinspectie Digitale Infrastructuur. Compliance certificates have a validity of two years, so the IPSP undergoes recertification audits every other year. In the other years, the IPSP is subject to surveillance audits. Additionally, internal audits are performed regularly.

6.2 Idenitty/Qualifications of Assessor

Cleverbase is certified by a conformity assessment body that is accredited as described in Article 2 of Implementing Regulation (EU) 2025/2162.

6.3 Assessor's Relationship to Assessed Entity

The external auditor performing the compliance audit functions independently from Cleverbase.

6.4 Topics Covered by Assessment

The Identity Proofing Service is in scope of the compliance audit.

6.5 Actions Taken as a Result of Deficiency

If, unexpectedly, deviations are found, a Corrective Action Plan is drafted to correct the deviations. The Corrective Action Plan is agreed upon with the external auditor and is given to the disposal of the Rijksinspectie Digitale Infrastructuur and the PA PKIoverheid.

6.6 Communication of Results

Compliance audit certificates can be consulted on the Cleverbase website: https://cleverbase.com/en/legal/qualifications. The underlying audit reports are confidential; they are confidentially shared with the Rijksinspectie Digitale Infrastructuur and the PA PKIoverheid.

7 Other Business and Legal Matters

7.1 Fees

7.1.1 Identity Proofing Fees

Any applicable fees are stipulated by the Product Conditions. If fees apply, they are communicated with Subscribers upfront.

7.1.2 Access Fees

No access fees apply. Subscribers can access results as part of a GDPR request as stipulated in the privacy statement.

7.1.3 Termination Fees

No termination fees apply.

7.1.4 Fees for Other Services

No compensation is required for the provision of information on the Identity Proofing Service. Only if exceptional efforts are required to answer an information request, reasonable costs can be charged. In such a case, the requester of this information is informed about the costs before committing to any expenditures.

7.2 Financial Responsibility

7.2.1 Insurance Coverage

The IPSP shall not be liable for any damage caused by the IPSP, unless in cases and insofar as described in Article 13 of Regulation (EU) 910/2014 (eIDAS) and its amendment Regulation (EU) 2024/1183. The IPSP's general terms and conditions contain the same limitation of liability. In order to cover this liability, the IPSP has arranged liability insurance covering up to at least 2,500,000.- euros.

The IPSP is not liable if Identity Proofing is not used as described in its IPSP and Product Conditions.

7.3 Confidentiality of Business Information

7.3.1 Scope of Confidential Information

The IPSP considers all data provided within the framework of the identity proofing service as confidential.

7.3.2 Information Not Within the Scope of Confidential Information

Information that is publicly available and cannot be linked to an identifiable person is not considered confidential.

7.3.3 Responsibility to Protect Confidential Information

Any party with confidential information at its disposal is responsible for ensuring its confidentiality.

7.4 Privacy of Personal Information

The IPSP has an Information Security Management System (ISMS) in place, ensuring confidentiality of personal data processed by the IPSP. The IPSP's Privacy Statement is applicable to all the provided services.

7.4.1 Privacy Plan

Please refer to the Cleverbase Privacy Statement available on the public website.

7.4.2 Information Treated as Private

Please refer to the Cleverbase Privacy Statement available on the public website.

7.4.3 Information Not Deemed Private

Please refer to the Cleverbase Privacy Statement available on the public website.

7.4.4 Responsibility to Protect Private Information

Please refer to the Cleverbase Privacy Statement available on the public website.

7.4.5 Notice and Consent to Use Private Information

Please refer to the Cleverbase Privacy Statement available on the public website.

7.4.6 Disclosure Pursuant to Judicial or Administrative Process

Please refer to the Cleverbase Privacy Statement available on the public website.

7.5 Intellectual Property Rights

All documents, products and services made public by the IPSP are subject to the IPSP's copyright and/or its suppliers/licenses. The IPSP indemnifies clients against claims by third parties regarding possible violations of intellectual property rights by the IPSP.

7.6 Representations and Warranties

The IPSP warrants that it: 1. observes the procedures described in this IPSP; 2. has performed all reasonable actions in order to ensure that data collected for Identity Proofing is correct at the moment of verification; 3. will deactivate a Subscriber's profile if it presumes that the data collected under Identity Proofing is not or no longer accurate

7.7 Disclaimers of Warranties

No limitations of warranties apply other than those mentioned in Section 7.6.

7.8 Limitations of Liability

No limitations of liability apply other than those mentioned in Section 7.2.

7.10 Term and Termination

7.10.1 Term

The IPSP's IPSPS becomes effective immediately after publication in the public repository and remains effective until a new version is published.

7.11 Individual Notices and Communications With Participants

The IPSP can be contacted via mail, electronic mail, and telephone. The IPSP publishes information on its public website and contacts individual subjects via electronic mail or telephone if applicable.

7.12 Amendments

7.12.1 Procedure for Amendment

Amendments to this IPSPS are made using the pre-defined, regular procedures for changing components of the I PPS services.

9.13 Dispute Resolution Provisions

If a dispute arises between the IPSP and a customer, or between the IPSP and a third party, the IPSP's management, having heard all involved and considered all interests at stake, decides. Such a decision is written down and delivered within a reasonable period of time. This procedure does not limit the possibility to submit disputes to the civil court in The Hague.

9.14 Governing Law

All the IPSP's activities are subject to Dutch law.