DIGIDENTITY

# Terms & Conditions

## Digidentity Identity Services

| | |
|---|---|
| **Title** | Terms & Conditions – Digidentity Identity Services |
| **Date** | 25 March 2019 |
| **Valid from** | 12 April 2019 |
| **Version** | 2019-v1 |
| **Classification** | Public |

## 1. About Digidentity

a) Digidentity B.V. is a registered limited company in The Netherlands, with company number 27322631, located at Waldorpstraat 17P, 2521 CA, The Hague, The Netherlands.

b) If you have any questions about the identity service, you can visit our website www.digidentity.eu or contact us via:

Reception: +31 (0)887 78 78 78
Service Desk NL: +31 (0)887 78 78 88
Service Desk UK: +44 (0)330 05 83 454
or
Dutch service desk: helpdesk@digidentity.eu
English service desk: helpdesk@digidentity.co.uk

## 2. Contract & Scope of Application

a) Digidentity delivers products and services for identity management and verification of identity. Digidentity is a Trust Service Provider for the issuance and management of EU qualified and advanced certificates, email certificates and server certificates.

b) These are the Terms & Conditions Digidentity B.V. These Terms & Conditions are applicable to all products and services delivered by Digidentity.

c) These Terms & Conditions are the foundation of the binding agreement between you (person or organisation) and Digidentity B.V. The Terms & Conditions exclude any other Terms & Conditions. In addition to these Terms & Conditions you may be required to accept product specific Terms & Conditions. These will be made available to you during the registration/application process where applicable.

d) These Terms & Conditions will apply to all aspects of the relationship and the contract between you and Digidentity, unless Digidentity has otherwise expressly agreed to in writing. Unconditional acceptance and agreement of these Terms & Conditions is implied.

e) Before being able to register for a product and/or service, you need to read and explicitly agree to these Terms & Conditions. To legally accept these Terms & Conditions you must have reached the legal age in your country of residence. This means that you are able to legally enter a binding contract.

f) The Terms & Conditions will continue to apply whether or not the application process, and/or verification of your identity, is successful.

g) Digidentity reserves the right to modify these Terms & Conditions at all times. The modified version will apply as soon as Digidentity has published them on the website. Once the Terms & Conditions change you will be required to read and accept them on your next use of your account.

h) If you are not in agreement with any modified or revised Digidentity Terms & Conditions, you can no longer use the Digidentity Identity Services. In that case you can contact the Service Desk who can arrange the deactivation of your account. You can reactivate your account within 30 days after deactivation by logging in and accept the Digidentity Terms & Conditions. After 30 days, your account is deleted.

## 3. Our Service

a) When you register for any product, you will need to register for an account. The process of verification will begin upon beginning registration and includes the validation and verification of the documents and data that you, and other sources, have provided.

b) To complete the registration process, you will need to submit all of the data required. If you do not supply all of the required data it will not be possible to verify your identity and/or organisation, and we will be unable to provide you with the product you require.

c) If the registration process is successful then Digidentity will make the product available to you via use of/or within your account, and the registration process will be complete.

d) If the registration process results in no confirmation and/or no verification, the application will be rejected, and the product will not be made available to you.

e) The decision to approve or reject applications for Digidentity's products and services remains for Digidentity B.V. at all times.

## 4. Products

a) At Digidentity, you are able to register/apply for the products listed on our website, to which these Terms & Conditions apply.

b) The use of our service is described in these Terms & Conditions, product specific Terms & Conditions and our Certificate Practice Statement.

## 5. Product Validity

a) For GOV.UK Verify accounts it is necessary to revalidate users within 180 days of first registration. If this revalidation is successful then no further validation will take place, and the account will remain active unless a request for deactivation or deletion has taken place. During the revalidation process GOV.UK Verify users may be asked to provide a new identity evidence.

b) For eHerkenning accounts the initial contract is for twelve (12) months. After twelve (12) months have passed, the account is automatically renewed for twelve (12) months and can be cancelled on a monthly basis.

c) SSL/SBR Certificates from the PKIo Private root are valid for three (3) years. Once the Certificate has expired a new application will be required. Digidentity do not extend existing Certificates but will issue new ones.

d) SSL Certificates from the PKIo public root are valid for two (2) years. Once the Certificate has expired a new application will be required. Digidentity do not extend existing Certificates but will issue new ones.

e) For eSGN Certificates (Qualified and Advanced) the initial contract is twelve (12) months. After twelve (12) months have passed, the account is automatically renewed for twelve (12) months and can be cancelled on a monthly basis.

f) For Profession Certificates initial contract period is for twelve (12) months. After twelve (12) months have passed, the account is automatically renewed for twelve (12) months and can be cancelled on a monthly basis.

g) Accounts and/or contracts cannot be transferred. Applicants, personal or organisational, must register for their own account.

## 6. Notice to Relying Parties

a) Digidentity recommends that relying parties verify the validity or revocation of the certificates using the current revocation status information.

b) Digidentity recommends that relying parties take account of any limitations on the usage of the certificate indicated either in the Terms & Conditions, Certificate Practice Statement or in the certificate itself.

c) Digidentity recommends that relying parties take the precautions prescribed in agreements and elsewhere.

d) Digidentity recommends that relying parties check the validity of certificates via the complete certificate chain to the trusted root certificate.

## 7. Personal Data Verification

a) To register an account, you will be asked to provide evidence of your identity. The evidence that you provide will be used to verify your personal data. The evidence requested can include;

i. Identity document via the mobile app – Passport or National Identity Card
ii. Selfies via the mobile app
iii. A zero-cost credit card/debit card transaction (UK)
iv. Your mobile phone number
v. A face-to-face meeting with a Digidentity representative
vi. Your email address
vii. Your home address (for GOV.UK Verify)
viii. Your date of birth
ix. Your address history (for GOV.UK Verify)
x. Your name history (for GOV.UK Verify)
xi. Your professional registration number for certificates for Registered Professionals.

b) Digidentity will only request the data which is required to create and verify your identity.

c) From time-to-time, Digidentity are required to perform revalidation of your existing data via the relevant issuing authorities. This is necessary to ensure that Digidentity have up-to-date and accurate information for the purposes of identity verification.

d) Any issued authentication certificate is not to be regarded as a form of legal identification document per the WID (Wet Identification – Dutch Law of Identification). Legal identification can only be shown by providing a recognised ID document.

e) Digidentity verifies the request for a certificate for Registered Professionals with the Nederlandse Beroepsorganisatie voor Accountants (NBA).

## 8. Organisation Verification

a) If your registration/application is on behalf of an organisation, or with authorisation of an organisation then Digidentity will request the following evidence/information, where applicable;

i. The Dutch Chamber of Commerce Registration Number (Dutch KvK Number)
ii. Organisation address details
iii. Organisation email address
iv. Validation of the Fully Qualified Domain Name (FQDN)
v. Blacklist/phishing list check
vi. Identity document copy of owner/director/legal representative
vii. Authorisation for the person applying for the certificate
viii. Letter to confirm employment of the person applying

b) Digidentity will only request the data which is required to verify the organisational identity and legal representation.

c) Digidentity will not issue certificates and/or other products if the organisation is in bankruptcy proceedings, or no longer registered at the Dutch Chamber of Commerce.

d) Digidentity will only issue certs to legal representative(s) with appropriate authorisations to enter a contract on behalf on an organisation.

e) If the Dutch Chamber of Commerce registry shows joint legal representation, then Digidentity will request authorisation from all legal representatives listed in the registry, without exception.

f) Any issued authentication certificate is not to be regarded as a form of legal identification document per the WID (Wet Identification – Dutch Law of Identification). Legal identification can only be shown by providing a recognised ID document per the WID.

## 9. Certificate Acceptance

a) The certificate is deemed to have been accepted by the subscriber once a period of more than one (1) calendar month has passed without any communication being received from the subscriber (person or organisation), or, that the certificate has been downloaded, used and/or installed.

## 10. Deactivation, Deletion and Revocation

a) You can deactivate your account at any time using the 'Deactivate my account' link in your account. A 30-day period deactivation period is started, as set out in our Certificate Practice Statement. You will not be able to use your account or the products in your account.

You can reactivate your account by logging in within 30 days after deactivation. If you have not reactivated your account within those 30 days, your account and all personal data will be deleted, and all certificates issued to you will be revoked. Relevant records will be kept for compliance purposes, in accordance with appropriate laws.

b) You can delete your account at any time by using the 'Delete my account' link in your account. Digidentity will permanently delete your account and personal data from our systems. Any certificates that have been issued to you will be revoked. Relevant records will be kept for compliance purposes, in accordance with appropriate laws.

c) If certificates have been issued to you, you can revoke these certificates by logging into your identity account and clicking 'Revoke certificates'. Once you have clicked this link, you will have to provide your password for authentication. Next, you will see an overview of all two factor authenticators and your personal certificates. You can revoke the relevant certificate by clicking 'Delete smartcard and revoke certificates' alongside the corresponding smartcard. Revocation will occur immediately, and you will no longer be able to use your certificate.

d) You may request revocation of your SSL/SBR certificate by logging into your SSL/SBR account and clicking 'revoke' alongside the corresponding certificate. Revocation will occur immediately, and you will no longer be able to use your certificate.

e) Digidentity reserves the right to deactivate accounts with immediate effect if there is any reason to believe or suspect that the verification and/or validation provided is no longer correct, or has been faulty, false or fraudulent as set out in the Certificate Practice Statement. If you want to continue using an account, you will need to apply for a new account.

f) Digidentity reserves the right to revoke any certificate if there is any violation of these Terms & Conditions, or any contractual agreement, or that Digidentity discovers that the certificate has been used, is being used, or will be used for any criminal activities, including phishing, fraud or for the distribution of malware/viruses.

g) Once a certificate is revoked or expired you may no longer use the private key associated with it.

h) Digidentity will refer any fraudulent activity to the relevant authorities. On behalf of the Identity service, we may also report any suspicious activities to any relevant body or appropriate authority.

i) Digidentity reserves the right to deactivate accounts with immediate effect if it considers communications from a user to Digidentity employees to be harassing, threatening, abusive. As far as Digidentity is concerned, this makes it impossible to provide reasonable services in support of applications for a digital identity. Digidentity will report any continuation of abusive, threatening or harassing behaviour to the appropriate authorities.

## 11. Our Obligations

a) Digidentity will provide the services as described on the website, in accordance with the Terms & Conditions, the Privacy Statement and Certification Practice Statement. Digidentity will carry out any contractual obligations. However, these obligations are no guarantee for a successful outcome in your application.

b) Digidentity aims to provide a continuously functioning and accessible service but makes no guarantees about the availability of any services provided. You accept the fact that (temporary) disruptions may occur which would render the service inaccessible on occasions.

c) Digidentity aims to make a documentation repository available 24 hours a day, 7 days a week. Should this repository become unavailable, Digidentity aims to recover its availability within four (4) hours.

d) Digidentity reserves the right to limit availability to or render the services entirely inaccessible for limited periods of time in order to carry out maintenance and/or implementation of required modifications. Digidentity aims to carry out these scheduled down times in periods which could be reasonably considered to affect the minimum number of users as far as possible, e.g. outside of office hours.

e) Digidentity will provide the service in accordance with the published Digidentity Privacy Statement. This Privacy Statement is accessible on the website. Digidentity will update its Privacy Statement from time to time to reflect changes to data processing in relation to the service.

## 12. Your Obligations

a) You understand that verification of identity is a process that relies on personal data, available documentation and information provided by you, and is uniquely based on your data. You accept that this identity verification process cannot be based on other user experiences or requirements.

b) You ensure and warranty to take all reasonable measures to assure control of, keep confidential, and protect the private key which corresponds to the public key of your issued SSL/SBR certificate. As a personal subscriber, you ensure the private key is under your sole control. As an organisational subscriber (legal subscriber) you ensure the private key is under the control of the subject.

c) You accept that unauthorised use of the subject's private key is forbidden.

d) You ensure and warrant to install the SSL/SBR certificate only on servers that are accessible at the subjectAltName listed in the certificate, and only to use the certificate in accordance with all applicable laws, agreements and Terms & Conditions.

e) You are obliged to report without any reasonable delay any suspected misuse, actual misuse or compromise of your certificate to Digidentity, and to immediately request revocation of the certificate.

f) You are obliged to notify Digidentity, without delay, if the private key has been lost, stolen or potentially or actually compromised, and to immediately and permanently stop use of this key, excepting key decipherment.

g) You are obliged to notify Digidentity, without delay, if control over the private key has been lost due to theft, compromise or loss of the activation data e.g. PIN code.

h) You accept your obligation for the key pair to only be used in accordance with any limitations notified. You also accept the obligation to only use the private key for cryptographic functions within the secure cryptographic device.

i) You ensure and guarantee that all data and documents provided are correct, complete, accurate and up-to-date, and that they conform to the requirements as set out by Digidentity during the registration process and application. You will update your online profile if changes occur in the data you have submitted upon registering. For SSL/SBR certificates you must inform Digidentity of any changes which cause a mismatch in your certificate information. You will follow instructions and requirements for any transfer of data (via the online process or using the mobile/tablet application) that Digidentity indicates.

j) You agree to inform Digidentity without delay if there are any security concerns, security issues or data leaks. Digidentity will treat any report as confidential and will handle it in accordance with appropriate laws and regulations to minimise damages. Digidentity aims to resolve any security alert as fast as reasonably possible and will take steps to inform any third parties that the issue affects.

k) You accept the obligation to inform Digidentity of any violation of the Terms described in articles 12, c) and 15, adding a detailed description of such violation and any other relevant information. You must take all reasonable measures to prevent further and/or continuing violations and will take all reasonable measures to limit any damage resulting from such a violation.

l) You accept the obligation to pay the invoice from Digidentity within fourteen (14) days after the issue date of the invoice.

## 13. Limitations of Use of our Website

a) It is forbidden to copy, pass on, sell, publish or make a profit from any content of the website, products, services or associated materials of Digidentity.

b) It is forbidden to use the website, products or associated materials of Digidentity in any way that causes, or may cause, damage to the website or impairment of the performance, availability or accessibility of the website, products or associated materials.

c) It is forbidden to access the Digidentity website and associated materials using any robot, spider or other means.

## 14. Personal Data

a) You acknowledge that Digidentity supply an identity, authentication and authorisation service and you understand that Digidentity will process personal data to establish an identity and to verify the validity of personal data or documents. Digidentity is the Data Controller as defined under the EU General Data Protection Regulation (GDPR) and will process the personal data with due care, in compliance with any applicable data protection laws including the GDPR, and these Terms & Conditions, unless otherwise agreed upon.

b) Digidentity processes the personal data in order to perform its duties under the contract with you and to create and maintain a direct relationship with you as indicated in the Privacy Statement. For the avoidance of doubt: this includes comparing and checking the data against databases (public or otherwise) that are available for the purpose. Digidentity will not process the personal data for other purposes, unless the processing is required on the basis of a legal obligation or a co urt order, or if you have given your consent.

c) In order to perform its duties under the contract, Digidentity will involve relying parties in the processing of personal data. Digidentity will take appropriate measures to ensure that these relying parties will process personal data in accordance with the purpose and applicable data protection laws.

## 15. Confidentiality

a) Digidentity and you are obliged to take all reasonable measures to protect confidential information or the identity account from unauthorised access, loss, damage, modification or unauthorised processing. In the event that such an issue occurs, you must inform Digidentity without delay of any unauthorised access, loss, damage, modification or unauthorised processing.

## 16. Record Retention

a) Digidentity may retain the following information (once registration is successful) during the lifetime of the account;

   i. Name
   ii. Address
   iii. Date of birth
   iv. ID document information: name, date of birth, nationality, document number, expiry date
   v. Mobile phone number
   vi. Email address

   All other data which has been used for verification during registration will be destroyed after fourteen (14) days.

b) Once deletion is confirmed, the account data is archived in an encrypted state for seven (7) years. Access to the archive is only given to authorised senior personnel, and only provided upon the requirement to provide evidence e.g. court proceedings. The archive remains locked under all other circumstances.

c) Digidentity will keep an event log of information having been received per account, which includes the receipt of data, the processing thereof and the outcome. These event logs are kept for the same period as the account data – seven (7) years once the account is deleted.

## 17. Rights of Ownership and Intellectual Property

a) At all times, any intellectual property rights that have to do with the identity service, or associated materials remain the property of Digidentity, the licensee or our supplier.

b) Your right to use the identity service or associated materials does not entitle you to any intellectual property rights of the identity service or associated materials. Digidentity only provides a non-exclusive right to use the identity service and/or associated materials to verify your identity and create an account. Your usage rights are strictly personal and cannot be transferred to any other person.

c) It is forbidden to use (part of) the identity service, data or associated materials in any way that would result in the violation of intellectual property rights of Digidentity, the licensee or suppliers.

d) Digidentity reserves the right to take all necessary measures to protect their own, the licensee's or suppliers' intellectual property rights. These measures include ending the use of the identity service

or associated materials when the contract ends. It is forbidden to use, remove or avoid any such measures in any way.

## 18. Liabilities

a) Nothing in these Terms & Conditions excludes or limits our liability in respect of

   i. any breach of law by Digidentity or its sub-contractors,
   ii. any loss, unauthorised access to or corruption of personal data held by Digidentity or its sub-contractors (including any credentials issued to you),
   iii. any wilful default on the part of Digidentity or its sub-contractors.

b) We are not responsible to you for any loss or damage suffered by you which was not an obvious consequence of us breaching these Terms & Conditions. We are not responsible to you for losses which you suffer due to any events beyond our reasonable control. We are not responsible to you for losses that that Digidentity has not caused directly by actions.

c) You cannot hold Digidentity liable for damages resulting from events beyond reasonable control or that Digidentity has not caused directly by actions.

d) You cannot hold Digidentity liable for any indirect damages or damages that were/or are caused because you did not/or do not take appropriate measures to:

   i. limit such damages immediately after a damaging event has occurred,
   ii. prevent further damage or subsequent damages resulting from the initial event,
   iii. immediately inform Digidentity about events which would cause damages and/or provide relevant information to Digidentity.

e) In all cases, the liability of Digidentity shall be limited to the usual and foreseeable damages. You cannot hold Digidentity liable for any business damages after using the identity service in the capacity of a consumer.

f) You can never hold Digidentity liable in respect of any damages resulting from

   i. Your unauthorised or improper use of the data, the identity service and/or related materials;
   ii. Providing incorrect and/or incomplete data, or not providing data to Digidentity in a timely manner;
   iii. Losing your own data;
   iv. Your failure to abide by any obligations provided in these Terms & Conditions or CPS, including not cooperating with the Terms & Conditions.
   v. The late, incorrect, or incomplete accessibility of the identity service;

vi. Miscommunication or loss of messages and notices resulting from the use of a mode of communication selected by you, or resulting from the dysfunction of any materials used by you, including improper functioning of the internet;
vii. The use of materials you selected;
viii. The unauthorised use, loss or theft of log in details that have been provided to you;
ix. The downtime or unavailable online tools of third parties;
x. Sharing your username, password or PIN code with any other person.

## 19. Limitation of Action

a) You must bring any claim for damages against Digidentity within one year after the damage has occurred.

## 20. Force Majeure

a) Digidentity is not obliged to perform any of the obligations under the contract or the Terms & Conditions in case of force majeure. Force majeure is understood to be a turn of event which is out of the reasonable control of the affected party, and therefore, if Digidentity cannot perform actions associated with, and not limited to;

i. Improper functioning materials provided by users
ii. Requirements under law
iii. Power cuts, power outages, or other interruptions of electricity
iv. Improper functioning of internet, computer and or telecommunication resources
v. Extreme weather Conditions, flooding, earthquake or other natural or weather-related causes;
vi. Strike, riots or civil unrest
vii. Fire or explosion
viii. War, uprising or overt military hostilities;
ix. Catastrophic epidemic or pandemic
x. General problems of transportation
xi. Extreme circumstances which reduce/severely limit the availability of Digidentity employees to carry out tasks
xii. Contradictory legislation or government action, prohibition, embargo or boycott
xiii. Terrorism
xiv. Failure of suppliers

Digidentity take measures to thwart the risk of any interruption to services, and have a business continuity plan and disaster recovery plan.

## 21. Applicable Laws, Regulations and Audits

a) The contract and the Terms & Conditions are governed by Dutch law in adherence and conformity with application European Directives, specifically Article 8 of the European Convention of Human Rights regarding laws on privacy.

b) Digidentity is audited and approved for the issuance, management and revocation of Qualified Certificates for electronic signatures per Regulation no. 910/2014 (EU), known as eIDAS.

c) Digidentity is audited annually against the requirements of ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, CA/Browser Forum Baseline Requirements, CA/Browser Forum Network Security Requirements, PKIoverheid Programma van Eisen, Afsprakenstelsel eHerkenning, tScheme and ISO27001:2013. Current certification can be viewed via this link: https://www.digidentity.eu/nl/home/#certifications

## 22. Complaints

a) Digidentity has a complaints procedure available, which can be viewed via this link: https://www.digidentity.eu/en/home/#complaints-procedure

b) Any dispute that a user and Digidentity cannot settle amicably will be brought before the competent judge of the place where Digidentity have a statutory seat (The Hague). If applicable Dutch or European law provisions determine that another judge is also competent, then the case may also be brought before this judge. If applicable Dutch or European law provisions determine that another judge has exclusive competence, then the case may only be brought before that judge.

## 23. Warranties

a) Digidentity does not provide for any other guarantees, undertakings, and/or commitments than those explicitly provided for in the Terms & Conditions.

## 24. Concluding Provision

a) Should any provision of the Terms & Conditions be declared invalid or void, this shall not affect the validity of any of the other provisions included in the Terms & Conditions. In such case Digidentity will amend the Terms & Conditions with the aim to achieve the same object and purpose served by the provision declared invalid.

## Definitions

The following words have the following meaning:

- **User**

  'User', 'you' or 'your' in these Terms & Conditions refer to you as a user of the Identity Service.

- **Identity service**

  The service we provide to you entailing the verification of your identity and/or the validity of any documents or data. If this verification and/or validation process results in a confirmation and/or validation of the information you have provided, we will create an identity account for your personal use.
- **Relying party**

  The relevant third party who requires you to verify your identity so that you can use its services, i.e., Government Departments.
- **Contract**

  The relationship between you and us, governed by the Terms & Conditions according to article 1.
- **Terms & Conditions**

  These Terms & Conditions as set out here.
- **Identity account**

  Your unique profile we have provided to you after identification and/or validation of data and documents whether or not the verification of your identity is successful
- **Data**

  Any data you have provided to us or in connection with the Digidentity Service.
- **Licensee**

  The holder of a licence for intellectual property rights connected to the identity service.
- **Materials**

  Materials refer to any software, hardware, websites, database, designs, models, programs, reports, and other identity services and materials we or the relying party have put to use in relation to the identity service.
- **In writing**

  For the present Terms & Conditions, the term ‘in writing’ will refer to any written communication, whether this be by electronic means or by regular postal mail.