

## Privacy Statement (12 April 2019)

At Digidentity, we respect your privacy and we are committed to protecting your personal data. In this Privacy Statement, we will inform you about the personal data we collect and process and how we protect your personal data.

### WHO ARE WE?

This Privacy Statement describes Digidentity B.V.'s collection and use of personal data. References in this Statement to "Digidentity", "we" or "us" shall mean Digidentity B.V. (registered in the Netherlands under company number 27322631), being the data controller for the data processing.

### WHAT IS THE PURPOSE OF THIS STATEMENT?

With every service we provide, we take the protection of your privacy and personal data seriously. We ensure that we collect and process personal data for the services provided and in compliance with applicable privacy and data protection law (including but not limited to the EU General Data Protection Regulation (GDPR)).

We do not allow anyone to use or access your personal data for any other purposes than those set out in this Statement.

In this Statement, we give you information about how Digidentity collects and processes your personal data when you visit our website or otherwise interact with us. This includes any personal data that you provide when you purchase our products or services. The Statement also informs you how you can exercise your rights.

It is important that you read both this Privacy Statement and our Terms & Conditions. This Privacy Statement does not override earlier policies, but rather supplements them.

### HOW CAN YOU CONTACT US?

If you have any questions, comments or requests concerning this Privacy Statement, please contact our Data Protection Officer (by e-mail, postal service or phone) using the details set out below.

Email address: [privacy@digidentity.com](mailto:privacy@digidentity.com)

Postal address: P.O. Box 19148, 2500 CC, The Hague, the Netherlands

Telephone number: +31 88 7 78 78 78

If you have any concerns about the way we handle your personal data, you have the right to make a complaint at any time to the data protection authorities. For Digidentity, this is the Autoriteit Persoonsgegevens in the Netherlands.

## **FOR WHICH PURPOSES DO WE USE YOUR PERSONAL DATA?**

### **Execution of contract**

Digidentity processes personal data for delivering our products or providing our services. The legal ground for processing personal data is to execute the contract with you for these products and services and to comply to applicable laws and regulations.

### **Legitimate interest**

Based on our legitimate interest, we process personal data to administer and protect our business and website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).

### **Consent**

We use automated technologies and interactions (including, but not limited to log data and data analytics and cookies). You can subscribe to our free newsletter by entering your email address. You can unsubscribe any time via link provided in the newsletter. In eSGN, you may give consent to use your location to fill in the name of the location in the signature location field.

## **WHICH PERSONAL DATA DO WE COLLECT?**

We process personal data when you interact with us, or when you use or purchase our products or services.

Digidentity process personal data and other data for providing our services which includes, if relevant:

### **Digidentity Account**

To use our services and products, a Digidentity account is required. For a Digidentity account, an email address is required, and you must create a password (minimum ten characters with at least one uppercase, one lowercase character and one number). Your email address and password are needed to access your account. A pseudonym is created to identify your account within our systems.

### **Level of Assurance 0**

Digidentity products that provide a Level of Assurance 0 (LoA0), require:

(1) **eSGN Basic:** your email address (as provided in your Digidentity account)

(2) **IVAS Level 0:** your email address (as provided in your Digidentity account)

### Level of Assurance 1

Digidentity products that provide a Level of Assurance 1 (LoA1), require:

(1) **eHerkenning Level 1:** your email address (as provided in your Digidentity account) and a business email address. If applicable, an employment letter is required stating that you are employed at your organisation and an authorisation letter is required stating you are authorised to act on behalf of your organisation. The full name of legal representative(s) of organisation, business address and business role(s) which we obtain from the Chamber of Commerce (KvK). We also request copy of ID document of legal representative(s) of organisation for signature verification.

(2) **GOV.UK Verify (Level 1):** your email address (as provided in your Digidentity account), phone number, full name, current and previous names, gender and addresses (minimum of one year of name and address history). Based on your name and address history, your UK credit file is checked in order match your details, as well as to generate Knowledge Based Verification (KBV) questions. We may also use your mobile phone number to verify a mobile contract attached to it. If the KBVs are attempted and failed, an app upload of a valid ID document is required for verification.

### Level of Assurance 2/2+

Digidentity products that provide a Level of Assurance 2 or 2+ (LoA2/2+), require:

(1) **eHerkenning Level 2+:** we request the same personal data as for eHerkenning Level 1 with the addition of mobile phone number to add two-factor authentication and a copy of ID document (for full name, date of birth and nationality verification)

(2) **GOV.UK Verify (Level 2):** we request the same personal data as for GOV.UK Verify Level 1 with the addition of three years of name and address history, active history in your credit file, plus one or more ID documents to prove who you are. If you verify a document using the Digidentity app on your mobile device, you must provide pictures of your ID document and selfies (of you) in order to compare the photo on the ID document with the selfies. When you provide the details of your ID documents using a manual form, we verify the data using the Document Checking Service (GOV.UK approved databases from DVLA, DVA and the UK Passport Office).

### Level of Assurance 3 or Substantial

Digidentity products that provide a Level of Assurance 3 (LoA3) or Substantial Level, require:

**(1) eSGN Advanced:** we request your email address (as provided in your Digidentity account), mobile phone number, full name, date of birth and gender. We need a copy of an ID document and three pictures (selfies) taken with the Digidentity app on your smartphone in order to compare the photo on the ID document with the selfies. We use the ID document to verify your full name, date of birth, place of birth and nationality and complete your registration.

**(2) eHerkenning Level 3:** we request the same personal data as for eSGN Advanced with the addition of business information. This includes registration number at the Chamber of Commerce, business email address, full name of legal representative(s) of organisation, copy of ID document of legal representative(s) of organisation (for identity verification), business address and business role(s).

An employment letter is required stating that you are employed at your organisation. If applicable, an authorisation letter is required stating you are authorised to act on behalf of your organisation. To finish the eHerkenning Level 3, we are required to perform a face-to-face verification of your identity.

**(3) IVAS Level 3:** we request the same personal data as for eSGN Advanced.

**(4) Solera Garage:** we request the same personal data as for eSGN Advanced.

### Level of Assurance 4 or High

Digidentity products that provide a Level of Assurance 4 (LoA4) or High Level, require:

**(1) eSGN Qualified:** we request the same personal data as for eSGN Advanced.

**(2) eHerkenning Level 4:** we request the same personal data as for eHerkenning Level 3.

**(3) Professional Certificates:** we request the same personal data as for eSGN Qualified with the additional request for your registration number from the Professional Registrar, your business email address and registration number at the Chamber of Commerce (for invoicing).

For all Level 4 products, we are required to perform a face-to-face verification of your identity. You will receive a request for a face-to-face meeting where Digidentity will verify your identity in person by checking the original ID document that you have uploaded during registration.

### Server certificates

Digidentity server certificates products, require:

- (1) **SSL/SBR:** your business email address (certificate manager, contact person), mobile phone number and registration number at the Chamber of Commerce, full name of legal representative(s) of organisation, copy of ID document(s) of legal representative(s) of organisation (for identity verification), business address and business role(s).

### Other products

For other products, Digidentity requires:

- (1) **ZLM:** your email address (as provided in your Digidentity account), insurance number and date of birth. Your insurance number and date of birth are sent to ZLM for verification. If the data is correct, we receive the email address registered at ZLM.
- (2) **Allianz:** your email address (as provided in your Digidentity account), your Digital Passport and Allianz registration number. The Allianz registration number and Digital Passport data are verified with Allianz. After approval of the application, Digidentity receives the name, date of birth and gender from the Digital Passport issuer Solera.
- (3) **Solera MMM:** your email address (as provided in your Digidentity account), name and a copy of an ID document.
- (4) **Smartr365:** your email address (as provided in your Digidentity account), name and a copy of an ID document.

### Digidentity website

We use cookies and Google Analytics on our websites:

- (1) **Cookies:** Cookies are files that store information on your device. We use cookies to provide you our services and products. These cookies are required for our products or services to work properly. We use cookies to analyse the use of our websites so we can improve performance, navigation and website experience. These cookies never store personal data. You can delete all cookies currently stored on your device. You can find out how to delete cookies for your browser by clicking 'Help' in your browser's menu.
- (2) **Google Analytics:** Digidentity uses Google Analytics to monitor and analyse the use of our website. We have set up Google Analytics to anonymise your IP address. We collect only anonymised data to improve our website, products and services.

### Digidentity Mobile App

The Digidentity mobile app (for Apple iOS and Android) may be used in the registration process, supports authentication and provides access to your virtual smartcard. The mobile app requests access to the camera of your mobile phone to allow scanning of QR codes. Your name is displayed on the virtual smartcard. If you enable analytics in the mobile app, we collect anonymised data on the use of our mobile app.

### **HOW DO WE USE YOUR PERSONAL DATA?**

Digidentity use your personal data to execute the contract that you have entered with us.

We are required by laws and regulations and international standards for digital identities to verify all personal data provided to make sure that your data is correct. Your email address and phone number are verified by sending a conformation code so we can verify you are in possession of the email address and phone number. We may use your mobile phone number and email address to contact you in relation to the product or service that you use.

We verify your full name, date of birth and nationality using a copy of your ID document. Your age is determined from you date of birth to verify you are of legal age for entering a contract us. During the registration, you are requested to upload a copy of both front and back of a valid ID document.

Digidentity use an external automated document validation system that checks if the ID document is genuine and valid. These automated validation check if all information is present and according to requirements (document valid, picture present, social security number passes the verification check). Documents that have been modified or data is hidden will be rejected. We collect your full name, date of birth, place of birth, gender, nationality and ID document number from your ID document as prove of verification. Your full name and nationality are included into digital certificates issued to you.

For professional certificates, we verify your registration at the Professional Registrar using your registration number to make sure you are eligible for a professional certificate.

During registration, three pictures (selfies) must be taken which we will compare to the picture on the ID document to verify your identity. The copies of your ID document and three selfies will be permanently deleted after 14 days. Credit file data (GOV.UK Verify) is deleted after 30 days.

### **HOW DO WE SECURE YOUR DATA?**

Digidentity has taken the necessary security measures to protect your personal data against accidental loss, unauthorised access, modification or disclosure. We limit access to your personal data to those employees who have a business need. They will only process your personal data as per our instructions, and they are legally bound to keep your personal data confidential.

We have set up procedures to deal with any suspected personal data breaches, and we will notify you and any relevant data protection authority of a breach where we are legally required to do so.

We have an Information Security Management System (ISMS) and are ISO27001:2013 certified. As part of our certification, our security measures to protect your personal data are annually evaluated by an external auditor. Digidentity is subject to regular inspections by Agentschap Telecom for Trust Services and Electronic Identification which also includes compliance to GDPR.

### **WHAT ARE YOUR RIGHTS?**

You have the right to:

- request information on personal data we process and what we do with the personal data
- request access to your personal data
- request correction of your personal data
- request erasure of your personal data.
- object to specific processing of the personal data
- revoke your consent

When you make use of your right, we are required to verify your identity. You can access, correct or erase your personal data in your account profile. In case we rely on your consent for the processing of your data, you have the right to revoke your consent at any time.

Please note that any processing we carried out before the withdrawal of your consent remains lawful. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case when you withdraw your consent.

If you wish to exercise any of these legal rights, please contact us via the contact information.