

Privacy Statement

Personal Data @ Digidentity

Title	Privacy Statement - Personal Data @ Digidentity
Date	8 October 2024
Valid from	15 October 2024
Version	2024-v2
Location	https://www.digidentity.eu/en/documentation/
Classification	Public



At Digidentity, we respect your privacy, and we are committed to protecting your personal data. In this Privacy Statement, we will explain how we collect, process and 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 Trade Register with registration 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 the collection and processing of personal data for the products provided is 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 provide you with information about how Digidentity collects and processes your personal data during any interaction with us or while on our website (www.digidentity.eu). This includes any personal data provided upon purchasing our products. The Statement also informs you on how to exercise your rights.

It is important that you read both this Privacy Statement, our General Terms & Conditions and any Product specific Terms & Conditions.

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 contact details set out below.

E-mail address:	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 register a complaint at any time to the data protection authorities. For Digidentity, this is the Autoriteit Persoonsgegevens (AP) in the Netherlands.

For which purpose do we use your personal data?

[1] Execution of Contract

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

[2] Legal Obligation

Digidentity processes personal data in compliance to legal obligations such as tax obligations, court orders or police investigations.

[3] Legitimate Interest

Based on our legitimate interest, we process personal data to administer, improve and protect our business and website. This includes troubleshooting, data analysis, testing, fraud prevention and detection, system maintenance, support, reporting and hosting of data.

[4] Consent

We use automated technologies and interactions (including, but not limited to log data, data analytics and cookies. In case we rely on your consent for the processing of your data, you have the right to revoke your consent at any time.

In compliance with GDPR article 9, sub 2a, we will ask you to give one-time explicit consent to Digidentity to process photos of your identity document and selfies (biometric data).

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

Which personal data do we collect?

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

Digidentity processes personal data for:

- Administration and invoicing
- Identification, identity validation & verification
- Delivery of products
- Improvement of products
- Fraud prevention & detection
- Analytics & Statistics
- Comply to laws and regulations
- Customer relation management
- Training purposes
- Contact purposes
- Sending newsletters
- Handling job applications

Digidentity process personal data which may include:

- Full name
- Previous names
- Date & Place of Birth
- Gender
- Nationality
- Identity documents (photo, chip)
- Photo read from chip & Selfies (biometric data)
- Address history
- E-mail address
- Business e-mail address
- Business registration
- Bank account number
- Identity document number
- Personal Identification Number
- Signature
- Mobile phone number
- Curriculum Vitae
- Motivation letter

Digidentity Account

To use products, a Digidentity account is required. The legal ground for processing personal data is to execute the contract. For a Digidentity account, an e-mail address is required, and Digidentity requires a second factor for authentication. When you register using the Digidentity Wallet, an authenticator with a pin code will be added to your account as second factor.

Your e-mail address and second factor are required to access your account. A pseudonym is created to identify your account within our systems. Digidentity stores this data until you delete your account, or for a maximum of two (2) years after the last time you logged in to your account. We will then assume that you no longer wish to use our products and will delete your account.

Delivery of products

Digidentity processes personal data to deliver our products. The legal ground for processing personal data is to execute the contract with you for these products and to comply to applicable laws and regulations. For example, we may process your full name, date of birth, place of birth, nationality, identity documents, images, and identity document number to verify your identity.

For our products, we are required to identify our customers. Digidentity processes photos of identity documents and selfies (biometric data) as part of identification of our customers. The purpose of processing biometric data to identify a customer, is to provide a digital identity to access services and systems.

Contact

When you use our products, send us an e-mail, fill out a contact form, or contact us in any other way, you accept our offer to contact you. The legal ground for processing personal data is legitimate interest. For this purpose, we may process your full name, e-mail address, mobile phone number and any data you enter yourself in the message content. We store this information until we are sure that you are satisfied with our response and one (1) year thereafter. This way we can access the data in case you have any follow up questions.

Digidentity Wallet

The Digidentity Wallet (for Apple iOS and Android) may be used in the registration process, supports authentication and provides access to your authenticator(s). The Wallet requests access to the camera of your mobile phone to allow scanning of QR codes and the NFC reader to read the chip on the identity document. Your name is displayed on the authenticator in your Wallet. If you enable analytics in the Digidentity Wallet, we collect anonymised data on the use of our Wallet. You can enable or disable displaying your profile picture in the Wallet.

Handling job applications

Have you responded to one of our vacancies or submitted an open application? If so, we will process your personal data in order to process your application and in preparation for the possibility of an employment contract. The legal ground for processing personal data is to execute the contract. For this purpose, we may process your curriculum vitae, motivation letter and any other data you enclose within your application.

We will retain your application details for a maximum of four (4) weeks after the position has been filled. We keep this data to contact you in the event that the position becomes vacant. If we are unable to offer you a job at this time, we may - with your consent – keep your application details for a year. You are able to withdraw your consent at any time by sending us an e-mail. If an employment contract is set up, we will save your application data in the personnel file.

A social media and internet check can be part of the application procedure. We do this on the basis of our legitimate interest. For this purpose, we search your name on the internet and, if necessary, your public profile(s) on social media. If applicable, the findings of this social media and internet check will be discussed with you. If you object to this, it is possible to indicate this by e-mail at the time of your application.

How do we use your personal data?

Digidentity uses your personal data for the delivery of products and to execute the contract that you have entered with us.

As per the laws, regulations and international standards for digital identities, we are required to verify all personal data provided by the applicant to ensure the data is correct. Your e-mail address and phone number are verified using a conformation code in order to verify that you are in possession of the e-mail address and phone number provided. We may use your mobile phone number and e-mail address to contact you in relation to the product that you use.

We verify your full name, date of birth and nationality using your identity document. Your age is determined from your date of birth. This verifies that you are of legal age to enter a contract with us. During the registration, we require photos of both front and back of a valid identity document and/or using the chip (NFC) within the document.

To check if an identity document is genuine, valid, lost or stolen, Digidentity uses external automated document validation systems. These automated validations check if all data is present as per the requirement (document valid, picture present, personal identification number passes the verification check). Documents which have been modified or missing/hiding data will be rejected because of the modifications. We collect your full name, date of birth, place of birth, gender, nationality and identity document number from your identity document as proof of verification.

Digidentity performs a face comparison of the selfies and the photo from the identity document to determine if the person on the document is performing the identity proofing process. Digidentity uses face comparison ('Is this the same person?'), not face recognition ('Who is this person?').

For sole contractors using eHerkenning, we must process your BSN to receive a pseudonym from the Dutch government required to access the Dutch tax office. Digidentity deletes your BSN as soon as the product is completed.

For UK Trust Framework, we may use your mobile phone number to match your personal data with your mobile provider. We send your name and address(es) to a Credit Reference Agency and request details of your credit history as part of the verification process as required by UK Trust Framework.

For products under the Digital Identities and Attributes Trust Framework (Right to Work, Right to Rent, Disclosure and Barring Service), the personal information we have collected will be shared with fraud prevention agencies who will use it to prevent fraud and money laundering. If fraud is detected, you could be refused certain services, finance, or employment. Further details of how your information will be used by us and these fraud prevention agencies, and your data protection rights, can be found by www.cifas.org.uk/fpn.

For registered profession certificates, we match your registration at the Profession Registrar using your registration number to make sure you are eligible for a profession certificate.

During registration, pictures (selfies) must be taken. We will compare the selfies to the picture on the identity document to verify your identity. We retain the photo from the chip or cropped photo from the front to perform re-identification. You may be asked to retake selfies which we compare to the photo on file to determine you are the holder of the account.

Digidentity performs several validation and verification steps to confirm your identity. In case fraud is detected, we reject your identity claim and register a fraud indicator. This could result in refusal of Digidentity products.

Digidentity uses external service providers to verify identity documents, perform liveness detection and face comparison, provide activity history and knowledge-based questions. We only share the necessary personal data which is necessary for these providers to perform their tasks. Digidentity also uses external IT suppliers and service providers.

Digidentity only shares your personal data with external parties when this is allowed as per applicable privacy and data protection law. Digidentity may provide personal data to external parties because:

- Digidentity has engaged external parties to process personal data
- it is necessary to execute the contract with you
- you gave permission for this
- Digidentity has a legitimate interest
- Digidentity is legally obliged to do so

Digidentity processes all personal data within the European Economic Area (EEA) and the United Kingdom. We do not sell or share your personal data to third parties or store your data outside the EEA. We only share personal data with third parties to comply to legal requirements.

Activity	Location Data Processing
Production systems	Ireland
Liveness Detection & Face Comparison	Germany, Ireland
Certificate Authority (CA) systems	Netherlands
Validation of identity documents	Netherlands, Ireland
Identity Fraud Check	Netherlands, United Kingdom

Digidentity uses automated decision making in the validation and verification of identity evidence. Our systems decide based on the results of validation and verification of identity evidence to accept or reject the identity claim. We always manually review rejected identity claims to prevent false rejections. We manually review automatically accepted identity claims based on random selection to prevent false acceptance of identity claims. We manually reject falsely accepted identities.

How do we protect your personal data?

Digidentity has taken the necessary security measures to protect your personal data against accidental loss, unauthorised access, modification, or disclosure. Digidentity uses the principles of “Privacy by Design” and “Privacy by Default” which means that protection of Personal Data was a default part of design of our systems.

Digidentity only collects personal data needed (data minimisation) and only processes for the identified purposes. We only process validated and verified personal data (data is checked against an authoritative source) to provide accurate digital identities. Digidentity creates a pseudonym for each account and use encryption to protect the personal data.

We limit access to your personal data to 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 a certified Management System for Information Security (ISO27001:2022) and Privacy Information (ISO27701:2019). As part of our certification, our security measures to protect your personal data are annually evaluated by an independent external auditor. Digidentity is subject to regular inspections by RDI (Dutch Authority for Digital Infrastructure) for Trust Services and Electronic Identification which also includes compliance to GDPR.

How long do we keep your personal data?

Digidentity must retain personal data for quality purposes and comply to laws and regulations. We implemented the following data retention periods.

Data	Retention Period
Verified Personal Data & photo from chip, cropped photo from front document	Active during contract, archived for seven (7) years after account deletion
Identity verification & validation reports	Active during contract, archived for seven (7) years after account deletion
Photographic evidence (identity documents, selfies)	Deleted after 45 days, unless consent of user is provided to retain for a longer period
Social Security Number or BSN	Deleted after completion of registration
PKI Key Life Cycle data	Active during contract, archived for seven (7) years after account deletion
Organisation data	Active during contract, archived for seven (7) years after account deletion
Accounts not used in last 24 months	Deleted after 45 days
Accounts with incomplete registration	Deleted after 45 days
Accounts that have no service purchased	Deleted after 45 days

Digidentity only allows access to archived personal data if required to meet obligations for auditing and forensic evidence purposes. During archival the data is securely stored (encrypted and masked). Data will only be accessible to personnel in functions related to security e.g. Security Officer or the Data Protection Officer (DPO). After the retention period of seven (7) years is reached, the archive is deleted/destroyed. The destruction of data ensures that no data can be recovered.

What are your rights?

You have the right to:

- request information on personal data we process and what we do with personal data
- request access to your personal data
- request correction of your personal data
- request erasure of your personal data
- request to transfer your personal data (if technically and/or legally possible)
- object to specific processing of the personal data
- revoke your consent

When you make use of your rights, we are required to verify your identity. You can exercise your rights to access, correct or erase your personal data or revoke consent in your account profile. You can log into your account at www.digidentity.eu.

Information on executing your rights is available on in our document "Data Subject Access Right @ Digidentity" on our website at: <https://www.digidentity.eu/documentation>.

Digidentity supports data portability. You can download your personal data from within your Digidentity account.

Digidentity reserves the right to update this Privacy Statement. New versions will be published on our website. We advise you to regularly check our website for any available update.

Digidentity protects your personal data and implemented a management system for security and privacy which has been certified against ISO27001:2022, ISO27017:2015, ISO27018:2019 and IS27701:2019.



Note: All changes in this document from the previous version are highlighted in grey.