

# QuoVadis Privacy Notice – Digital Certificates and Signing Solutions

This QuoVadis Privacy Notice relates to the services provided by QuoVadis for the issuance of digital certificates and the provision of signing solutions. For Swiss certificate and signing solutions provided by QuoVadis Trustlink Schweiz AG (QVTLISAG) please see our separate privacy notice [here](#).

We take your privacy seriously and will only use your personal data to deliver the products and services requested.

## Who are we?

QuoVadis is an EU Qualified Trust Services Provider. QuoVadis provides services using a group of wholly owned subsidiaries. The following QuoVadis entities are relevant to the provision of digital certificates and signing solutions:

- QuoVadis Trustlink B.V. (Netherlands)
- DigiCert Europe Belgium BV (Belgium)
- QuoVadis Trustlink Deutschland GmbH (Germany)

The above entities are Controllers of personal data in relation to the provision of our products and services. All DigiCert Group entities comply with the provisions of this Privacy Notice.

## Who are our Privacy Officers?

Our Data Privacy Officer is Aaron Olsen (email: [privacy@digicert.com](mailto:privacy@digicert.com)).

## What data is collected?

We collect the data necessary for the provision of the services we provide.

### Certificate Content

Personal data that may be included in Personal Digital Certificates can include:

- First Name
- Last Name
- Pseudonym (if applicable)
- Common Name
- E-mail address
- Title (e.g., Mr./Mrs./Dr.)

- Job title (professional title)
- Company/Organization name (if applicable)
- Company/Organization legal identifier (if applicable)
- Organizational Unit (if applicable)
- Serial number (if applicable)
- Address attributes (if applicable)
- Government issued ID document number (e.g., passport, driving license). Only if explicitly requested by the customer.

### **Registration Data**

Personal data that is not included in Personal Digital Certificates but that may be requested as part of the Certificate issuance process (e.g., for verifying the identity of an individual). This data can include:

- Address
- Telephone number
- Identification document details (used for identity verifying)
- Company registration details and validation of authority

### **Account Data**

Personal data is also needed to create a user account on our certificate management systems or in our signing solutions. This personal data consists of:

- First Name
- Last Name
- Username (chosen by user)
- Email address
- Telephone number
- Password (chosen by user)
- Mobile number
- PIN and/or One-Time Password secret

Certain Digital Certificates such as device certificates do not contain any personal data, but personal data may be requested as part of the application for such certificates including the name, title, email address and telephone number of the relevant people involved with the certificate request and approval process.

Individuals registering with remote identity verification should consult our privacy notice [here](#).

Note that we do not obtain the documents to be signed, only a cryptographic hash of the document is received. Our signing solutions do log the use of the system and the details of the document signings that take place.

## **Why do we collect information? / Lawful Basis for processing**

We rely on a variety of information to run our business. In some cases, this information may include data that relates to an identified or identifiable natural person, which is referred to as personal data.

The reason that we collect your personal data is that we need it to provide you with our products and services, which include the provision of digital certificates and signing solutions.

The lawful basis for us processing personal data in relation to these services is that processing is necessary for the performance of a contract or to take steps to enter into a contract (in the case of customers who are natural persons) or as it is in our legitimate interest and the legitimate interest of our customers to provide our services to our customers, which services require processing of natural-person representatives of our customers (in the case of customers who are legal entities). Individuals registering with remote identity verification should consult our privacy notice [here](https://www.quovadisglobal.com/accreditations/)<https://www.quovadisglobal.com/accreditations/>.

## **Who is collecting it?**

We collect data directly from you or indirectly from those organizations who have entered into a contract with us (for example to request certificates for their employees). We may also use third-party agents to collect data from you (for example, as a service to verify an ID document). Where we use such third parties they act entirely under our control and serve as a data processor. They do not retain your data or use it for any purpose other than to provide it to us.

## **How will it be used?**

We use your personal data only for the provision of the products and services that we have contracted to provide.

## **Who will it be shared with?**

We do not share your personal data with anyone except to deliver the agreed services.

On occasion, data might be shared within the DigiCert Group to ensure adherence to audit and compliance regulations on an as needed basis or with respect to escalations. Phone number might be sent to an international SMS-provider to send OTP's (One-Time Password) as part of the signature process if requested by our customers.

## **Where will it be stored?**

Personal data provided for the use of digital certificates and electronic signatures as part of our EU Certificate and Signing Solutions is stored within the European Economic Area (EEA).

Information retained in our office includes contracts, customer contact information, and verifying information that supports the issuance of digital certificates. This applies to hard copy physical documents and electronic data.

## How is your data protected?

We use a combination of technical, administrative, organizational and physical safeguards to protect your personal data. Access to your personal data is restricted to those who are necessary for the delivery of the services. These safeguards are tested as part of our annual audits and accreditations. For further details please see details of our [accreditations](#) and [technical and organizational measures](#).

## Retention Periods

The QuoVadis Certification Policy/Certification Practice Statement (available at <https://www.quovadisglobal.com/repository>) requires that audit logs relating to the certificate lifecycle are retained as archive records for a period no less than eleven years for Swiss Qualified/Regulated Certificates and for seven years for all other Digital Certificates. Note that this period begins when the certificate expires.

## Your Rights

We comply with all relevant data protection and privacy legislation. These laws provide a number of rights with regard to your personal data.

You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time, which will not affect the lawfulness of the processing before your consent was withdrawn.

You have the right to lodge a complaint with the appropriate data protection authority if you believe that we have not complied with our legal obligations. For further information on EU data protection authorities please see [here](#). For further information on Swiss data protection authorities please see [here](#).

If you wish to exercise any of your rights as discussed above, please submit your request through our [Privacy Request Form](#); you may also email [privacy@digicert.com](mailto:privacy@digicert.com) if you have any questions.

## Automated Decision Making and Profiling

An automated decision is defined as a decision which is made following processing of personal data solely by automatic means, where no humans are involved in the decision-making process. Except in the single instant noted below, we do not use automated decisions in the processing of personal data. Individuals registering with remote identity verification should consult our privacy notice [here](#).

We do not engage in profiling.

## This Privacy Notice

As our organization grows, this Privacy Notice is also expected to change over time. This Privacy Notice may be updated periodically to reflect changes in our personal information practices. You should check our site frequently to see the current Privacy Notice that is in effect.

The Privacy Notice was last updated on 23 August 2022.

## Contact

If you have questions regarding this Privacy Notice, please contact us via email at: [privacy@digicert.com](mailto:privacy@digicert.com)