

# QuoVadis Privacy Notice – Digital Certificates and Signing Solutions

This QuoVadis Privacy Notice relates to the services provided by QuoVadis (“QV” or “QuoVadis”) for the issuance of digital certificates and the provision of signing solutions. QuoVadis is a member of the DigiCert Group, whose parent company is DigiCert, Inc., located in Utah, USA. 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. QV provides services using a group of wholly-owned subsidiaries. The following entities form part of this group and are relevant to the provision of digital certificates and signing services:

- QuoVadis Trustlink BV (Netherlands)
- QuoVadis Trustlink Schweiz AG (Switzerland)
- DigiCert Europe Belgium BV (Belgium)
- QuoVadis Trustlink Deutschland GmbH (Germany)
- QuoVadis Online Limited (United Kingdom)
- QuoVadis Limited (Bermuda)

The above entities are Controllers of personal data in relation to the provision of our products and services. Further details of these Controllers are [here](#). All QuoVadis companies comply with the provisions of this Privacy Notice.

## Who are our Privacy Officers?

Our Data Protection Officer is Aaron Olsen (email: [dpo@digicert.com](mailto:dpo@digicert.com) or [privacy@quovadisglobal.com](mailto:privacy@quovadisglobal.com)).

## What data is collected?

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

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

- First Name
- Last Name
- Common Name
- E-mail address
- Title (e.g. Mr./Mrs. /Dr.)
- Job title (professional title)
- Pseudonym (if relevant)
- Company/Organization name (if relevant)
- Organizational Unit (if relevant)
- Locality
- State/Province
- Country
- Government issued ID document number (e.g. passport, driving license). Only if explicitly requested by the customer.

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 vetting the identity of an individual). This data can include:

- Address
- Telephone number (home/mobile)
- Identification document details (used for identity vetting)
- Company registration number and data

Personal data is also needed in order to create a user account on our certificate management systems in order to log in to the system. This Personal Data consists of:

- First Name
- Last Name
- Email
- Phone number(s)
- Password (chosen by user)

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. The name, title, email address and telephone number of the relevant people involved with the certificate request and approval process.

Our signing solutions capture Personal Data as part of the user registration process. This Personal Data includes:

- Name
- userID
- Email address
- PIN and/or One Time Password secret
- Mobile phone number
- Identification document details
- Details to be included in the Digital Certificate, which is produced after registration process completed. See above for the data included in a digital certificate

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 in order to provide you with our products and services, which include the provision of digital certificates and signing services.

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).

## Who is collecting it?

We collect data directly from you or indirectly from those organisations 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 save to deliver the agreed services (see next paragraph).

Personal data provided as part of our services such as the certificate content and in some cases registration data, may be shared within the DigiCert Group in order to process the certificate.

In order to process digital certificates, we transfer certificate content information to QuoVadis Limited in Bermuda and to DigiCert, Inc. in Utah, USA. The reason for this is that our back-end certificate processing systems are located in Bermuda and the USA. This data is restricted to only the data that will be included in the digital certificate and the transfer takes place over an encrypted connection within our systems.

The European Commission has not currently provided an adequacy decision for Bermuda or for the USA. However, Bermuda does have privacy legislation in place, known as the Personal Information Protection Act (PIPA), 2016; likewise the USA has certain sectoral and regional legislation that is protective of individual privacy interests. Further safeguards are therefore necessary for this data transfer to Bermuda and to the USA to take place. These safeguards take the form of a series of intercompany agreements based on the Standard Contractual Clauses authorized under the European Commission Implementing Decision (EU) 2021/914, 4 June 2021.

Click [here](#) for the DigiCert Privacy Policy for more information on standards.

## 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](#).

## Retention Periods

The QuoVadis CP/CPS (available at <https://www.quovadisglobal.com/QVRepository.aspx>) requires that audit logs are retained for at least seven years. 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, 30 years for certificates issued out of Belgian Issuing CAs 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/ Privacy legislation. These 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 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@quovadisglobal.com](mailto:privacy@quovadisglobal.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 instance noted below, we do not use automated decisions in the processing of personal data.

The GDPR defines profiling as '*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*'. We do not perform any profiling.

Our remote identity verification process does involve use of automated decision making, wherein you use a mobile device with camera to compare your image to an uploaded ID document. The process is designed to verify your identity with reference to the ID document. If you wish not to use this automated process you are given the option to have a human agent verify your identity. You may also contact [privacy@quovadisglobal.com](mailto:privacy@quovadisglobal.com) or [support@digicert.com](mailto:support@digicert.com) if you have any concerns about the automated identity verification process or if you feel that the process has failed to analyze your image correctly.

## This Privacy Notice

As our organisation grows, this Privacy Notice is also expected to change over time. This Privacy Notice may be updated periodically and without prior notice to you 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 1 December, 2021.

## Contact

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