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.

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

WHO ARE WE?

QV is a Qualified Trust Service 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)
- QuoVadis Trustlink BVBA (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. The following page of our website provides further details of these Controllers:

https://www.quovadisglobal.com/Locations.aspx

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 or privacy@quovadisglobal.com).

Our Privacy Officers are:

- Main: Barry Kilborn
- Deputy: Rolf Gerritsen

email: 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.

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).

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 QuoVadis Group in order to process the certificate.

In order to process digital certificates, we transfer certificate content information to QuoVadis Limited in Bermuda. The reason for this is that our back-end certificate processing systems are located in Bermuda. 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. However, Bermuda does have privacy legislation in place, known as the Personal Information Protection Act (PIPA), 2016. Further safeguards are therefore necessary for this data transfer to Bermuda to take place. These safeguards take the form of a series of intercompany agreements based on the Standard Contractual Clauses authorized under the EU Data Protection Directive 95/46/EC and permitted under EU GDPR regulation 2016/679. To request a copy of these agreements please email privacy@quovadisglobal.com.

As much information as possible is retained in the local QuoVadis subsidiary that has the customer relationship. The information retained in this office includes contracts, client contact information and vetting information that supports the issuance of digital certificates. This applies to hard copy physical documents and electronic data. The table below summarises the QuoVadis entities and data flows.

QuoVadis Subsidiary	Country	EU Adequacy Decision?	Data transferred outside the country
QuoVadis Trustlink BV	Netherlands	N/A – in EU	For certain certificates issued by QuoVadis Trustlink BV, the certificate request portal is maintained in a data centre in Switzerland. When the applicant completes the initial certificate request the data to be included in the certificate is transferred via https to QuoVadis Trustlink Schweiz AG in Switzerland. Data to be included in a Digital Certificate (which can include Personal Data) is transferred to QuoVadis Limited in Bermuda for processing.
QuoVadis Trustlink Schweiz AG	Switzerland	Yes	Data to be included in a Digital Certificate (which can include Personal Data) is transferred to QuoVadis Limited in Bermuda for processing. For eIDAS EU Qualified Certificates, the application forms and vetting data that supports the issuance of certificates is sent to QuoVadis Trustlink BV in the Netherlands for secure storage.
QuoVadis Trustlink BVBA	Belgium	N/A – in EU	Data to be included in a Digital Certificate (which can include Personal Data) is transferred to QuoVadis Limited in Bermuda for processing. For eIDAS EU Qualified Certificates, the application forms and vetting data that supports the issuance of certificates is sent to QuoVadis Trustlink BV in the Netherlands for secure storage.

QuoVadis Trustlink Deutschland GmbH	Germany	N/A – in EU	Data to be included in a Digital Certificate (which can include Personal Data) is transferred to QuoVadis Limited in Bermuda for processing. For eIDAS EU Qualified Certificates, the application forms and vetting data that supports the issuance of certificates is sent to QuoVadis Trustlink BV in the Netherlands for secure storage.
QuoVadis Online Limited	United Kingdom	N/A – in EU	Data to be included in a Digital Certificate (which can include Personal Data) is transferred to QuoVadis Limited in Bermuda for processing. For eIDAS EU Qualified Certificates, the application forms and vetting data that supports the issuance of certificates is sent to QuoVadis Trustlink BV in the Netherlands for secure storage.
QuoVadis Limited	Bermuda	No	QuoVadis hosts CRL and OCSP certificate status validation services at a third-party provider. These servers are located in Frankfurt and Dublin. The data transferred as part of this process is transferred from Bermuda in an encrypted manner over a VPN and is restricted to data required to publish the status of the certificate (valid/revoked etc.).

We may share your personal data with DigiCert, Inc. ("DigiCert"), our parent company. One reason for this is that our systems are in the process of being integrated. Click here for the DigiCert Privacy Policy. Transfers to DigiCert are performed on the basis of intra-group agreements, which are based on the EU's standard contractual clauses for export of personal data to third countries.

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 the 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.

Please email privacy@quovadisglobal.com to make a request under these provisions. In order to help us deal with such request please provide details of the product/service that the request relates to, the relevant QuoVadis office/ contact person and any other details (such as customer number etc). Please note that we will perform steps to verify your identity before providing any information.

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. We do not use automated decisions in the processing of personal of 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.

The Privacy Notice was last updated on March 4, 2019.

CONTACT

If you have questions regarding this Privacy Notice, please contact us via email at: privacy@quovadisglobal.com.

Our Data Protection Officer can be contacted on dpo@digicert.com or privacy@quovadisglobal.com.