HydrantID Privacy Notice – Digital Certificates and Signing Solutions

This HydrantID Privacy Notice relates to the services provided by Avalanche Cloud Corporation dba HydrantID ("HydrantID") for the issuance of digital certificates and the provision of signing solutions.

HydrantID and all its affiliates (hereinafter referred to as "HydrantID," "we" or "us") are committed to maintaining the privacy of every current, former, and prospective customer. We recognize that you entrust important personal information to us, and we assure you that we take seriously our responsibilities in protecting and safeguarding this information. This HydrantID Privacy Notice describes in detail how we deal with information that we collect on this website (the "Site") and the iD Opener smartphone application (iDO).

The HydrantID Privacy Notice Highlights provides a shorter summarized version of the full HydrantID Privacy Notice, which can be found here and in the HydrantID Repository. It relates to the services provided by us 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?

HydrantID is the brand for Public Key Infrastructure (PKI) products (digital certificates and signing solutions) issued by Avalanche Cloud Corporation, dba HydrantID, and also issued on behalf of HydrantID by our affiliate partner Quovadis, the ultimate parent Company of which, Digicert is based in Utah.

See digivert + Quovadis Privacy Policy here: https://www.quovadisglobal.com/privacy-policy/

HydrantID and its affiliates comply with the provisions of this Privacy Notice.

Who are our Privacy Officers?

Our Data Protection Officer (DPO) is Rocky Taylor.

Our Privacy Officers are:

- Main: Rocky Taylor email: privacy@hydrantid.com

What Data are 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.)
- 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 are 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)
- Passport / Drivers license details (used for identity vetting)
- Date of birth
- Company registration number and data

Personal data are 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)

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 consists of:

- UserID
- PIN
- One Time Password secret
- Mobile phone number
- Digital Certificate (produced after registration process complete)

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 which includes login details, IP addresses and when the document signing took 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 data?

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).

How will data be used?

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

Who will data be shared with?

We do not share your personal data with anyone, except to deliver the agreed services described in the 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 HydrantID in order to process the certificate.

In order to process digital certificates, we transfer certificate content information to Quovadis in Bermuda. The reason for this is that the 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 HTTPS connection within our systems and Quovadis's 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@hydrantid.com.

As much information as possible is retained in the local HydrantID or 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 HydrantID and Quovadis entities and data flows.

Entity	Country	EU Adequacy Decision?	Data transferred outside the country
Amazon Web Services	Oregon USA	Yes – Privacy Shield	For certain certificates issued by HydrantID or QuoVadis Trustlink BV on behalf of HydrantID, the certificate request portal is maintained in a data center 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 Germany. Data to be included in a Digital Certificate (which can include Personal Data) is transferred to HydrantID in the USA or QuoVadis Limited in Bermuda for processing.
Amazon Web Services	Virginia USA	Yes – Privacy Shield	For certain certificates issued by HydrantID or QuoVadis Trustlink BV on behalf of HydrantID, the certificate request portal is maintained in a data center 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 Germany. Data to be included in a Digital Certificate (which can include Personal Data) is transferred to HydrantID in the USA or QuoVadis Limited in Bermuda for processing.
Amazon Web Services	Germany	N/A – in EU	For certain certificates issued by HydrantID or QuoVadis Trustlink BV on behalf of HydrantID, the certificate request portal is maintained in a data center 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 Germany. Data to be included in a Digital Certificate (which can include Personal Data) is transferred to HydrantID in the USA or QuoVadis Limited in Bermuda for processing.
Switch	Nevada USA	Yes – Privacy Shield	For certain certificates issued by HydrantID or QuoVadis Trustlink BV on behalf of HydrantID, the certificate request portal is maintained in a data center 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 Germany. Data to be included in a Digital Certificate (which can include Personal Data) is transferred to HydrantID in the USA or QuoVadis Limited in Bermuda for processing.
Equinix	Virginia USA	Yes – Privacy Shield	For certain certificates issued by HydrantID or QuoVadis Trustlink BV on behalf of HydrantID, the certificate request portal is maintained in a data center 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 Germany. Data to be included in a Digital Certificate (which can include Personal Data) is transferred to HydrantID in the USA or QuoVadis Limited in Bermuda for processing.

QuoVadis Trustlink BV	Netherlands	N/A – in EU	For certain certificates issued by HydrantID or QuoVadis Trustlink BV on behalf of HydrantID, the certificate request portal is maintained in a data center 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 HydrantID or QuoVadis Limited in Bermuda for processing on behalf of HydrantID. 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 HydrantID or QuoVadis Limited in Bermuda for processing on behalf of HydrantID. 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 HydrantID or QuoVadis Limited in Bermuda for processing on behalf of HydrantID.

			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 HydrantID or QuoVadis Limited in Bermuda for processing on behalf of HydrantID. 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	On behalf of HydrantID, QuoVadis Limited hosts CRL and OCSP certificate status validation services at a third-party provider. These servers are located in Germany and Ireland. 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.).

How data may be disclosed

We may disclose personal information that we collect or that you provide as described below:

- To contractors, service providers, and other third parties we use to conduct our business.
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution or other sale or transfer of some or all of Avalanche Cloud Corp's assets, in which personal information held by Avalanche Cloud Corp about our customers is among the assets transferred.
- For any other purpose disclosed by us when you provide the information.

- To comply with any court order, law or legal process, including to respond to any government or regulatory request.
- To enforce or apply our terms of use and other agreements, including for billing and collection purposes.
- If we believe disclosure is necessary or appropriate to protect the rights, property or safety of Avalanche Cloud Corporation, our customers, or others.

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 QuoVadis's annual audits and accreditations. For further details please see details of the QuoVadis accreditations.

Retention Periods

HydrantID retains information and audit logs for at least seven years or as specified in contractual agreements.

For certificates issued by Quovadis on behalf of HydrantID, the QuoVadis CP/CPS 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 may 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@hydrantid.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 HydrantID 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”.

Neither HydrantID or Quavids perform profiling.

Other Information We Collect

We may collect information about you when you use this Site or when you apply for or use other services offered by HydrantID in the following ways:

This website uses Google Analytics, a web analytics service provided by Google, Inc. (“Google”). Google Analytics uses “cookies,” which are text files placed on your computer, to help the website analyze how users use the site.

The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser. However, please note that if you do so, you may not be able to use the full functionality of this website. By using this website, you consent to the processing of data about you by Google in the manner and for the purposes set out above.

If you register to use the password-protected or country-specific portions of our Site, we will ask you to provide us with certain information about yourself. This information may include your name, company name, title, address, e-mail address and telephone number. We use such information about you to verify your identity in order to provide information to you about products and services that we believe may be of interest to you and to respond to your requests for information. We may also use cookies and "web bugs" on such portions of our Site to collect Usage Information, and to facilitate your movement within the Site.

We may also collect personal information about you from applications, forms, or questionnaires you may complete or agreements you enter into with us or in the course of your establishing or maintaining a customer relationship with us.

If you decline to provide us with the personal information we require, then we may not be able to grant access to certain website areas or send you the appropriate information.

Security of Data

HydrantID uses only encrypted HTTPS connections to transport personal data. Please note that data that is transported over an open network, such as the Internet or e-mail, may be accessible to anybody. HydrantID cannot guarantee the confidentiality of any communication or material transmitted via such open networks. We will not ask you to disclosure any personal

information other than from web pages that use strong HTTPS encryption to transfer your data. For this to be effective we recommend that you use an up-to-date Internet browser and update your computer regularly with security patches and updates from the applicable service provider.

Your data may be lost during transmission or may be accessed by unauthorized parties. We do not accept any liability for direct or indirect losses as regards the security of your data during its transfer via the Internet. Please use other means of communication if you think this is necessary or prudent for security reasons.

Personal Data Maintained by HydrantID

We restrict access to personal information about you to those employees, agents, or other parties who need to know that information to provide products or services to you or in connection with services you provide to us. We maintain physical, electronic, and procedural safeguards to guard your personal information, including firewalls, individual passwords and encryption and authentication technology. We do not use for purposes other than as set out above, or disclose to any third party, any personal information about our customers or former customers, except with such customer's consent or as otherwise permitted or required by law. In some cases, we may share your personal information with affiliates of HydrantID to the extent permitted by applicable law. We may also disclose this information to firms that perform services on our behalf, to the extent permitted by applicable law. These service providers are required to treat the information confidentially and use it only for the purpose for which it is provided. Certain jurisdictions may have more stringent privacy requirements that will prevent disclosure of your personal information to any other person or entity, including affiliates.

We will retain your personal information in accordance with applicable data protection laws, for so long as it is needed.

Links

This Site may contain hyperlinks to other websites that are not operated or monitored by HydrantID. These other websites are not subject to this Policy and we are not responsible for their content or for the policy they apply to the treatment of personal data. We recommend that you read the policy used by

these websites and check how these websites protect your personal data and whether they are trustworthy.

iD Opener Smart Phone Application

HydrantID publishes a smart phone application called iD Opener (iDO), which is used as a second-factor form of strong authentication to various websites and applications, known as “realms”. As such, iDO requires access to your personal or sensitive user data (including personally identifiable information, contacts, identity and authentication information, location, and camera sensor data), which is used to securely authenticate you to a realm.

All such data is transported only over the encrypted HTTPS protocol to each realm.

The camera sensor is used when you scan a QR Code, which is used with an optional PIN, to authenticate you a realm for which you are registered and authorized to access. GPS Location data may optionally be requested by the realm to which you are authenticating. This information, along with your identity information, is used to strongly authenticate you to a realm.

This Privacy Notice

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.

This Privacy Notice Highlights was last updated on March 30, 2020. The full HydrantID Privacy Notice Highlights provides a complete version of HydrantID’s Privacy Policy. The full HydrantID Privacy Notice can be found here in the HydrantID Repository

Contact

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