

ZENTRY LLC

PRIVACY NOTICE

Purpose and Scope of this Privacy Notice

This privacy notice (the “**Privacy Notice**”) describes how Zentry LLC and/or its local subsidiary/ies (as applicable) (“**Zentry**”, “**we**”, “**us**” and “**our**”) treat information about you that you may provide to us or that we may collect (“**Personal Data**”), including how we may use such information, how we protect the security of such information, the third parties to whom we share such information and what rights you have about the use of your Personal Data in particular the right to object to the processing of your Personal Data where that processing is carried out for our legitimate interests. The Personal Data we hold includes any information associated directly with you (such as your name, title, email address or phone number) that is supplied to us in conjunction with your use or potential use of our services, known as Universal ID or UID (hereafter “**UID**” or the “**Service**”) as well as information we generate regarding your use of the Service.

Please note this Service includes hyperlinks to other websites neither owned nor managed by us. Zentry is not associated with these third-party websites and does not review their privacy policies. We cannot guarantee the privacy of any information that may be obtained by third parties at these other websites. We strongly encourage you to review the privacy policies of any website you visit before supplying Personal Data through that website.

Click a link below for further information on each topic:

1. [What Personal Data does Zentry collect about users of its permission-based Service and how is this Personal Data used?](#)
2. [How does Zentry protect the security of the Personal Data I provide?](#)
3. [The third parties with whom Zentry shares information](#)
4. [What about the transfer of Personal Data to other countries?](#)
5. [How long does Zentry retain Personal Data?](#)
6. [What rights do I have about the use of my Personal Data?](#)
7. [How will I be notified of changes to this Privacy Notice?](#)
8. [How can I contact Zentry with questions about this Privacy Notice?](#)

1. What Personal Data does Zentry collect about users of its UID Service and how is this Personal Data used?

UID provides a cloud-based identity-as-a-service solution that includes identity proofing, credential issuance, strong authentication, and digital signature services. This Service shifts complexity from the organization’s IT Department to Zentry—allowing the organization to still retain control of access management. Services that take organizations weeks to perform can be handled in minutes - without paper-based processes or manual updates for multiple applications.

In summary, the UID solution provides:

- Cloud-based identity solution that helps reduce the risk of identity fraud by providing real-time transactional identity assurance;
- NIST Level 3 compliant ID Proofing and Authentication services on-demand identity-as-a-service, without the complexity and expense of on-premises hardware and software;
- Rapid-deployment, fast identity proofing and credential issuance;
- Positive user experience for credential provisioning and transactional authentication;
- Strong support for open standards, including SAML and OATH, to provide compatibility with third-party products and services; and
- Standard authentication experience across applications.

As a user of the UID, we will collect Personal Data:

from you: for example through the information you provide to us in setting up your UID profile, the Personal Data you supply via our website, email and telephone.

from third party sources: including Personal Data from provided by the Relying Party (typically your employer), software platforms we use for business processes, API, information from statutory and regulatory authorities, public notaries, trusted agents and occasionally some additional sources.

In delivering the UID solution, Zentry may capture the following Personal Data:

- a) First Name
- b) Middle Name
- c) Last Name
- d) Street Address
- e) City
- f) State
- g) Zip Code
- h) District
- i) Country
- j) Email address
- k) Phone/Cellphone Number

- l) Identification Info: Passport #, Driver's License #, other identification information such as Permanent Resident card #, National ID Card #; identifying document must not have expired and contain a photo
- m) Gender
- n) Username
- o) Employer Enterprise ID
- p) Birthplace
- q) Date of Birth
- r) Credit Card Account Number (Not retained; only used for IDP transmission)
- s) Bank Account number (Not retained; only used for IDP transmission)
- t) Social Security Number

We may also collect and process **Personal Health Information** about you and only to the extent permitted or required by applicable law or pursuant to a permitted justification under applicable law. The Personal Health Information we collect includes your DEA/Healthcare License Number (for clients enrolled in Healthcare vetting) and your Digital Certificate.

The following table details the legal basis for (the "**Legal Basis**") and the reasons why ("**Purposes**") we process your Personal Data:

NECESSARY FOR ENTERING INTO OR PERFORMANCE OF A CONTRACT	
Legal Basis	It is necessary to process your Personal Data to enter into and perform our contract with you and provide the UID Service.
Purposes	<p>We obtain, collect and process your Personal Data:</p> <p><u><i>Entering Into and Performing our Contract with you as a recipient of the UID Service:</i></u></p> <ul style="list-style-type: none"> • to determine, perform and execute the terms on which you will engage with us; • to ensure the smooth running of our relationship with you (including all of the activities that need to be undertaken before, during and after our contractual relationship); • to process any financial payments; and • to administer requests or procedures requested by you throughout our contractual relationship.

	<p><u><i>Identity Proofing & Credential Provisioning</i></u></p> <p>For the purpose of identity proofing and issuing credentials in particular:</p> <ul style="list-style-type: none"> • to confirm your identity and provide an identity proofing mechanism; • to verify your identity through our online antecedent process and enterprise antecedent data load; • to authenticate the information provided by you in the credential process against external information sources; and • to enable you to associate an issued credential with your devices. <p><u><i>Digital Signature Service</i></u></p> <p>For the purposes of offering our Digital Signature Service in particular:</p> <ul style="list-style-type: none"> • to provide a digital signature service that enables you to apply digital signatures to documents and Adobe PDFs. <p><u><i>UID Mobile Application</i></u></p> <p>For the purpose of managing and offering the UID Mobile Application in particular:</p> <ul style="list-style-type: none"> • to offer the UID Service in the form of a mobile application; • to provide a soft token that generates one-time passcodes; • to provide a QR code scanner service as part of the UID Mobile Application; and • to operate the UID Message Center function in the UID mobile application.
IMPORTANT	<p>You are obliged to provide us with your Personal Data as it is necessary to enter into a contract with us a user of the UID Service and enable us to provide our UID Service to you. In the event that you do not wish to provide us with your Personal Data for the above purposes, you will not be able to avail of the UID Service.</p>

LEGITIMATE INTERESTS	
Legal Basis	We may obtain, collect and process your Personal Data where we have a legitimate interest to do so.

Purposes	<p>We obtain, collect and process your Personal Data:</p> <p><u>Authentication</u></p> <p>For the purpose of providing an authentication service;</p> <ul style="list-style-type: none"> • to support flexible enterprise and user preferences for managing both first and second factor authentication; • to provide one-time passcodes within timeout and lockout policies; and • to limit organizational risks.
IMPORTANT	<p>When we process your Personal Data based on our legitimate interests, we make sure to consider and balance any potential impact on you and your data protection rights. We will not use your Personal Data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted by law).</p>

COMPLIANCE WITH A LEGAL OBLIGATION	
Legal Basis	<p>It is necessary to process your Personal Data in order to comply with legal obligations to which we are subject.</p>
Purposes	<p>We obtain, collect and process your Personal Data in order to comply with the following legal obligations:</p> <ul style="list-style-type: none"> • to comply with the Kantara Trust Framework (certified by the Federal Identity, Credential and Access Management program (FICAM)); • to comply with the SAFE-BioPharma Digital Identity and Signature Standard; and • To comply with other applicable laws.

2. How does Zentry protect the security of the Personal Data I provide?

We care about protecting your information and we are committed to keeping your Personal Data confidential. Zentry takes appropriate and reasonable precautions and has implemented appropriate administrative, technical and organisational procedures to protect the security of

information provided or generated through the Service. We require persons working for us to only access and use Personal Data in a manner consistent with this Privacy Notice.

3. The third parties with whom Zentry shares information

Zentry may disclose your Personal Data to third Parties (1) in response to a subpoena, search warrant, court order, exchange rule, other legal process or where Zentry is otherwise required to do so in accordance with locally applicable law and where applicable, our internal policy on access by government or regulatory authorities; and (2) if such disclosure is required in connection with an official government or regulatory investigation, or under exigent circumstances in response to a perceived significant threat to a person's health or property.

Zentry may also disclose some or all of the Personal Data to the following third parties:

- Internal teams within Zentry such as IT, Finance, managers, system administrators and support staff
- IT & website service providers, and other suppliers;
- Other people in your organisation;
- Third parties involved in verifying the Personal Data you provide to us in the identity proofing process e.g. notary public;
- Third parties in connection with the sale or purchase of Zentry or assets owned by Zentry; and
- Professional advisors such as tax or legal advisors, consultants and accountants.

4. What about the transfer of information to other countries?

Your Personal Data may be stored and processed in any country where we have facilities or in which we engage service providers, and by using our products and services (including the Service), you consent to the transfer of Personal Data to countries outside of the location(s) of your business, including the United States and countries within and outside the European Economic Area (“**EEA**”), which may have different data protection rules than those of your country.

Where such transfers of your Personal Data are made they will be made in accordance with applicable law. Where your Personal Data is transferred outside the EEA, this may include transfers on the basis of Standard Contractual Clauses, or as is otherwise permitted by applicable law. Standard Contractual Clauses are a form of data processing contract approved by the European Commission. You can find a copy of these clauses [here](#).

If you would like to find out more about any such transfers, please contact our Privacy Officer whose details are set out at section 8 of this notice.

5. How long does Zentry retain Personal Data?

In general, we expect to keep your Personal Data for a period of 7.6 years if you are a LOA1, LOA2, or LOA3 FICAM subscriber, or for a period of 9.6 years if you are a Digital Certificate subscriber. Once we have determined that we no longer need to hold your Personal Data, we will delete it from our systems.

Please note that in certain circumstances, we may hold your Personal Data for a longer period, for example, if we are processing an ongoing claim or believe in good faith that the law or a relevant regulator may reasonably in our view expect or require us to preserve your Personal Data.

If you would like to know more about how long we will retain your Personal Data, please contact our Privacy Officer whose details are set out at section 8 of this notice.

6. What rights do I have about the use of my information?

If the EU General Data Protection Regulation ("GDPR") applies for you, you have a number of rights in relation to your Personal Data which are set out in this section 6. **In particular these rights include the right to object to processing of your Personal Data where that processing is carried out for our legitimate interests.** Note that in certain circumstances these rights might not be absolute.

Right	Further Information
Right of Access	You have the right to request a copy of the Personal Data held by us about you and to access the information which we hold about you. We will only charge you for making such an access request where we feel your request is unjustified or excessive.
Right to Rectification	You have the right to have any inaccurate Personal Data which we hold about you updated or corrected.
Right to Erasure	In certain circumstances, you may also have your personal information deleted, for example if you exercise your right to object (see below) and we do not have an overriding reason to process your Personal Data or if we no longer require your Personal Data for the purposes as set out in this notice.
Right to Restriction of Processing	You have the right to ask us to restrict processing your Personal Data in certain cases, including if you believe that the Personal Data we hold about you is inaccurate or our use of your information is unlawful. If you validly exercise this right, we will store your Personal Data and will not carry out any other processing until the issue is resolved.

Right to Data Portability	You may request us to provide you with your Personal Data which you have given us in a structured, commonly used and machine-readable format and you may request us to transmit your Personal Data directly to another data controller where this is technically feasible. This right only arises where: (1) we process your Personal Data with your consent or where it is necessary to perform our contract with you; and (2) the processing is carried out by automated means.
Right to Object	You have a right to object at any time to the processing of your Personal Data where we process your Personal Data on the legal basis of pursuing our legitimate interests.

You can exercise any of these rights by submitting a request to our Privacy Officer by email at privacyofficer@zentry.com or by post to the following address:

Privacy Officer
 Zentry LLC
 200 Crossing Blvd.,
 Bridgewater,
 NJ 08807,
 USA

We will provide you with information on any action taken upon your request in relation to any of these rights without undue delay and at the latest within 1 month of receiving your request. We may extend this up to 2 months if necessary however we will inform you if this arises. Please note that we may ask you to verify your identity when you seek to exercise any of your data protection rights.

You also have the right to lodge a complaint about the way we handle or process your personal data with your national data protection regulator. For further information please see [here](#).

7. **How will I be notified of changes to this Privacy Notice?**

From time to time, we may change and/or update this Privacy Notice. Any changes will be effective immediately upon communicating the revised notice to you.

If at any time we decide to use your Personal Data in a manner significantly different from that stated in this notice, or otherwise disclosed to you at the time it was collected, we will notify you by e-mail, and you will have a choice as to whether or not we use your Personal Data in the new manner.

8. How can I contact Zentry with questions about this Privacy Notice?

If you have questions about this Privacy Notice and how we handle your Personal Data, please contact our Privacy Officer by email at privacyofficer@zentry.com or by post to the following address:

Privacy Officer
Zentry LLC
200 Crossing Blvd.,
Bridgewater,
NJ 08807,
USA