Privacy and Security Policy

At ISONAS, privacy and security are core elements of our service. Accordingly, we are always conscious and respectful of the privacy and confidentiality of individuals who visit ISONAS' websites ("Visitors"), individuals who use our products and services ("End Users"), individuals who develop applications using ISONAS' APIs ("API Partners") and individuals engaged in selling ISONAS' products ("Partners").

This Privacy Statement describes ISONAS' privacy practices in relation to the use of the Company's websites and the applications and services offered by ISONAS (the "Services"). By visiting our websites or providing us with your personal information, you consent to the collection, processing, and storage of your personal information as described in this Privacy Policy.

Websites Covered

This Privacy Policy covers the information practices of websites that link to this Privacy Policy including: ISONAS.com; pureaccessmanager.com; pureaccesscloud.com; isonaspureaccessmanager.com; isonaspureaccesscloud.com; isonaspureaccess.com; isonaspureaccessdemo.com, collectively referred to as ISONAS' websites.

ISONAS' websites may contain links to other websites. The privacy statements of those websites govern the information practices and the content of those websites. ISONAS encourages you to review the privacy statements of other websites to better understand their information practices.

Roles of Participants in Information Management

ISONAS provides products to End Users via its authorized Reseller channel. ISONAS' Partners handle the initial set-up and configuration of the ISONAS Pure Access application and hardware. End Users can choose what data to share with the Partner during the set-up process. After initial set-up, access to the End User's ISONAS Pure Access account is limited to authorized Administrators. ISONAS employees have access to End User data solely to provide our services and in response to specific customer requests for technical support.

Collection and Use of Information

From Visitors to our websites, ISONAS collects only the personal information necessary to enable us to respond to your requests for our products and services. When you visit our website, you may be asked to identify your product needs or the business category of your company, as well as your e-mail address, company name, business address and phone number. This information will better enable us to respond to your requests. If you wish to subscribe to news and information, we will use your address information for this purpose. We will provide you a way to modify your communication preferences and to unsubscribe.

As Visitors navigate ISONAS' websites, we may also collect information through the use of commonly used information-gathering tools, such as cookies and Web beacons ("Web Site Navigational Information"). Web Site Navigational Information includes standard information from your Web browser (such as browser type and browser language), your Internet Protocol ("IP") address, and the actions you take on our websites, such as the pages viewed and the links clicked. The information we collect from our websites (such as domain name, number of hits, pages visited, and length of user session) may be combined to analyze how our websites are used. This information is then used to improve the usefulness of the sites.

From End Users, ISONAS collects information (Customer Data) for the purposes of providing our services. We collect information in the following ways:

Information provided by End Users: ISONAS Pure Access provides the capability for End Users to store basic personal information such as an individual's name, email address and photograph. This information is used to correlate security events to the correct individual, as well as to enable notifications and ISONAS Pure Mobile functionality. Though the system has the capability to store a number of personal data elements, these items are not essential for operation of the system.

Information generated from events: ISONAS Pure Access collects access control event data. For example, ISONAS Pure Access records that an access card was used at a particular door at a certain time. Through correlation with the information our End Users provide, we can tie that access event to a particular individual's credential.

Log Information: ISONAS Pure Access records the actions of system Administrators, as well as the status and the settings of various devices that have been configured to operate with ISONAS Pure Access. Customer Data entered in ISONAS Pure Access by End Users or collected through the operation of the system are for the exclusive use of our End Users. ISONAS may access Customer Data only for the purposes of providing the functionality of the Products, preventing or addressing service or technical problems, or as may be required by law.

Third Parties: ISONAS shares data with relevant third party processors when explicitly authorized by Administrators in the relevant ISONAS Pure Access account; for example, to enable integrations via our Application Programming Interface (API) to Video Management Systems, Microsoft Active Directory, or other such programs.

Right of Individual Access and Limited Use: EU citizens may request access to or limited use of their personal data within the ISONAS system by submitting a request to: support@isonas.com or calling 303-567-6516.

Lawful Requests: ISONAS also may disclose Personal Data for other purposes or to other Third Parties when a Data Subject has consented to or requested such disclosure. Please be aware that ISONAS may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements. ISONAS is liable for appropriate onward transfers of personal data to third parties.

Customer Data may also be used by ISONAS to:

- Enable event notifications and ISONAS Pure Access functionality.
- Contact you to inform you of product and service enhancements that we think may be of interest to you.
- Provide important service notices regarding the ISONAS Pure Access application and related devices. While you use ISONAS products, it will not be possible to opt out of communications regarding service notices.
- Ask you to participate in surveys that help us better understand your needs in order to improve our products.

From Partners, ISONAS collects the personal information that is needed to properly manage our business relationship. ISONAS Partners will receive login credentials to manage End User accounts. Partners are able to create a new account for each End User by providing Account Name, Username, and Email address. We

only collect this information for the purposes of allowing you to manage your End User accounts and for the purposes stated above.

Data Location & Transfer of Information

ISONAS stores all Customer Data in the continental United States. To facilitate our End Users' global operations, ISONAS transfers information to the United States and provides access to that information to End Users around the world.

Data Safeguards

The security of Customer Data, including personal data, is very important to ISONAS. ISONAS maintains a comprehensive, written information security programs that contains industry standard, administrative, technical, and physical safeguards designed to prevent unauthorized access to Customer Data.

Data Retention

ISONAS retains Customer Data according to the timeframes set forth in the relevant service level agreement.

E.U.-U.S. Privacy Shield Statement
ISONAS, Inc. complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. ISONAS, Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

In compliance with the Privacy Shield Principles, ISONAS commits to resolve complaints about our collection or use of your personal information. Individuals in the European Union with inquiries or complaints regarding our Private Shield policy should first contact ISONAS at support@isonas.com or 303-567-6516.

If you do not receive timely acknowledgement of your complaint, or if your complaint is not satisfactorily addressed by ISONAS, EU individuals may bring a complaint before the BBB EU Online Privacy Shield. Information about how to file a complaint before the BBB EU Privacy Shield program can be found at: www.bbb.org/EU-privacy-shield/for-eu-consumers/.

The Federal Trade Commission (FTC) has jurisdiction over ISONAS' compliance with the Privacy Shield.

Deleting or Updating Information
ISONAS encourages you to contact us if you wish to delete, correct or update your business information in our systems, or if you desire to change your preferences with respect to marketing contacts from ISONAS by emailing us at support@ISONAS.com.

ISONAS reserves the right to change this Privacy and Security Policy. Any changes to this policy will be made to this Privacy Policy document, posted to www.isonas.com and will become effective immediately. Use of the ISONAS site constitutes consent to any policies then in effect.

Changes to this Privacy Statement

ISONAS reserves the right to change this Privacy Policy and will provide notification of the material changes to this Privacy Policy through the Company's websites at least thirty (30) business days prior to the change taking effect.

Capitalized terms in this Privacy Policy have the following meanings:

"Individual Customer" means an Individual customer or client of ISONAS from the EU. The term also shall include any individual agent, representative, of an individual customer of ISONAS and all employee of ISONAS where ISONAS has obtained his or her Personal Data from such Individual Customer as part of its business relationship with ISONAS.

"Data Subject" means an identified or identifiable natural living person. An identifiable person is one who can be identified, directly or indirectly, by reference to a name, or to one or more factors unique to his or her personal physical, psychological, mental, economic, cultural or social characteristics.

"Employee" means an employee (whether temporary, permanent, part-time, or contract), former employee, independent contractor, or job applicant of ISONAS or any of its affiliates or subsidiaries, who is also a resident of a country within the European Economic Area.

"Europe" or "European" refers to a country in the European Union.

"Personal Data" as defined under the European Union Directive 95/46/EC means data that personally identifies or may be used to personally identify a person, including an individual's name in combination with country of birth, marital status, emergency contact, salary information, terms of employment, job qualifications (such as educational degrees earned), address, phone number, e-mail address, user ID, password, and identification numbers. Personal Data does not include data that is de-identified, anonymous, or publicly available. For Switzerland, the term "person" includes both a natural person and a legal entity, regardless of the form of the legal entity.

"Sensitive Data" means Personal Data that discloses a Data Subject's medical or health condition, race or ethnicity, political, religious or philosophical affiliations or opinions, sexual orientation, or trade union membership.

"Third Party" means any individual or entity that is neither ISONAS nor an ISONAS employee, agent, contractor, or representative.

ISONAS Statement on GDPR Compliance

The EU General Data Protection Regulation (GDPR) is a data protection regime that becomes effective on May 25th, 2018. The GDPR extends the scope of the EU data protection law to all foreign companies processing data of EU residents.

The GDPR provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime.

ISONAS' Position:
At ISONAS, privacy and security are core elements of our service. Accordingly, we are always conscious and respectful of the privacy and confidentiality of individuals who visit ISONAS' websites, use our services, develop applications using ISONAS' APIs and resell ISONAS' products.

ISONAS maintains comprehensive, written information security programs that contains industry standard, administrative, technical, and physical safeguards designed to prevent unauthorized access to Customer Data. ISONAS does not share, sell, rent or trade personally identifiable information with third parties.

ISONAS has a strong track record of compliance with data privacy and security best practices. We have invested in the people, processes and technology to comply fully with the GDPR.

ISONAS participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework with respect to transfer of data to the US. We recognize that the GDPR will help us move towards the highest standards of operations in protecting customer data.

Application of the GDPR for ISONAS:

In the context of the GDPR, individuals with data stored in ISONAS Pure Access or individuals using ISONAS applications are considered Data Subjects. ISONAS end-users and in some cases ISONAS Resellers are considered Data Controllers. ISONAS is a Data Processor.

In ISONAS' role as a Data Processor, we are the responsible custodian of the Data Subject's data, performing this role on behalf of the Data Controller. The Data Controller is completely responsible to determine what data is captured, stored and processed within our application. The Data Controller is the owner of the data. ISONAS does not rent, share, disclose or sell any data owned by the Data Controller.

Within our service model, most Data Subjects will have no direct interaction with the ISONAS application that captures and stores their data. Most Data Subjects will be employees or contractors of the Data Controller. Data is captured based on their relationship with the Data Controller. The Data Controller is responsible for gaining explicit consent from the Data Subject regarding the data to be stored. Data Subject requests to purge data from ISONAS subject to ISONAS' SLA with the Data Controller will be adjudicated by the Data Controller.

In cases where Data Subjects use ISONAS' website or applications directly, ISONAS is the Data Controller and as such ISONAS will be responsible for gaining explicit or unambiguous consent based on the type of data collected. Data Subject requests to purge data collected directly by ISONAS will be adjudicated by ISONAS.

The GDPR includes provisions that grant Data Subjects portability rights in their personal data. Any personal data we store on behalf of Data Controllers is the Data Subjects. We will coordinate with Data Subjects and, as applicable Data Controllers, when requested to delete or port data. We provide for portability and are continually working to enhance our data export capabilities.

Summary

Privacy and security are core elements of ISONAS' services, so we are committed to the spirit and intent of the GDPR. While we have a solid data protection foundation in place, we recognize the need to make additional required operational changes resulting from the new legislation.

We will continue to monitor the GDPR and evolve our systems and processes to ensure continued compliance.

Contacting us

If you have questions or comments about the ISONAS Privacy and Security Statement, please feel free to contact us at privacy@ISONAS.com.