

PRIVACY & SECURITY NOTICE FOR SOFTWARE USERS

Seclore acknowledges the importance of safeguarding the privacy and security of your Personal Data (*defined hereinafter*) and is committed to upholding this responsibility. This Privacy & Security Notice for Software Users ("**Notice**") has been created to provide you with an understanding of how we process Personal Data, offering transparency and giving you the ability to access and control your Personal Data.

In this Notice, references to "**Seclore**", "**we**", "**us**", or "**our**" mean the Seclore entities which may Process your Personal Data. The relevant entities are listed in Exhibit 2 (*as amended from time to time*).

Seclore provides Enterprise Digital Rights Management Software and Services (collectively "**Seclore Product(s)**" or "**Product(s)**") to its customers to help them protect their organizations from cybersecurity threats and compliance risks. Your access to Seclore Products is facilitated through an organization (namely our customer), with which you are associated in some capacity. That organization as a Controller controls your use of the Product and the Personal Data that is transmitted to us for Processing.

By proceeding to use Seclore Products, you consent that we can Process the Personal Data that we may collect from you in accordance with this Notice.

INFORMATION THAT WE COLLECT

When you download and/or access the Seclore Product to access your Files, we have access to the following information (collectively "**Personal Data**"):

- User's name, email address.
- User's Internet Protocol (IP) addresses.
- User's Device name and Security Identifier (SID).
- User's Login identification.
- User agent type.
- User's Operating system.
- Date/time stamp of usage and activities performed with the File (access, close, edit, print, unprotect).
- User's device ID; and
- User's folder name

In case, any Personal Data is stored within the Files, such data is stored temporarily in Seclore's servers in encrypted form:

- For as long as configured by the customer / organization which facilitates your access and use of the Product.
- For as long as you access a File using agentless access and this File is automatically deleted as soon as you close the browser session.

In case we provide remote support Services to you, we may process the above-listed Personal Data in order to troubleshoot the incident and may be able to view Files open on your device. In order to ensure minimization of Processing, we recommend that you close all the Files that are not necessary for us to see when we provide support Services (for example, your emails, work documents unrelated to the issues requiring support).

PURPOSES AND LEGAL BASES OF PROCESSING THE PERSONAL DATA

a) Software Installation and Tracking Reports:

When you install the Product to have access to the Files, we as a Processor collect the Personal Data in order to enable the installation of the Product on your device, creation of your user account and to generate tracking reports and to ensure that any fixes, updates, and upgrades will be automatically generated on the Product in accordance with the Subscription Agreement executed with the customer. The legal basis for this processing is **contractual necessity**.

b) Usage Analysis and Improvement:

We use the collected Personal Data to analyze aggregate usage patterns and trends with the aim of enhancing user experience and gathering demographic information about our user base as a whole. The legal basis for processing is **legitimate interests**.

c) Support Services: Information collected during support Services helps us troubleshoot issues effectively. The legal basis for this processing is **contractual necessity**.

We do not use the Personal Data collected to contact you for marketing purposes nor do we sell such Personal Data to third parties.

Legal basis for processing Personal Data (EEA Users only)

If you are a User of our Product from the European Economic Area, our legal basis for collecting and using the Personal Data described above will depend on the Personal Data concerned and the specific context in which we collect it. In any case, we will generally collect Personal Data from you only where we have your consent to do so, where we need the Personal Data to fulfill contractual obligations for you, to comply with a legal obligation or where the Processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms.

HOW LONG WE KEEP YOUR PERSONAL DATA

We will keep your Personal Data only for as long as is necessary for the purposes for which we are processing it or as may be required under legal interests /compliance or contractual necessity. We will delete or otherwise destroy your Personal Data as soon as practicably possible following termination, cancellation, or stoppage of your use of the Product or through the effect of termination of the Subscription Agreement under which the Seclore Products were being provided (whichever is later).

WHO WE SHARE YOUR PERSONAL DATA WITH

We may share your Personal Data with your consent (provided herein) or the consent of the organization through which you are accessing the Products, to provision of your access or use of the Products.

- We may from time to time use certain third parties like business partners, suppliers, and sub-contractors) to carry out certain activities on our behalf that involve the Processing of Personal Data . This may include, but not be limited to, third party service providers or Sub-Processors to provide support Services or to provide the servers on which we host the data (such as Amazon Web Services) or implement Security Measures to protect your data. These third parties or Sub-Processors have access to Personal Data needed to perform their functions but may not use it for other purposes. In all such cases, we remain liable under applicable law for the processing of your Personal Data.
- We may share the Personal Data with the other Seclore entities, our consultants, counsels, and agents.
- We may disclose your Personal Data to government or law enforcement officials or private parties if we are under a duty to disclose or share your Personal Data in order to comply with any legal obligation (including in connection with a court order, or meet national security requirements), or in order to enforce or apply our terms and conditions , or respond to claims and legal process, or to protect our rights, property or safety or those of other users, our customers, employees or other third parties, or to stop any illegal, unethical or legally actionable activity (including for the purposes of fraud protection and credit risk reduction).
- In the event that we sell or buy any business or assets, we may disclose Personal Data held by us to the prospective seller or buyer of such business or assets. If we or substantially all of our assets are acquired by a third party (or subject to a reorganization within our corporate group), Personal Data held by us will be one of the transferred assets.

WHERE YOUR PERSONAL DATA WILL BE PROCESSED

Your Personal Data may be transferred to, and stored and processed in India, in the United States, in the European Economic Area ("EEA") or in other countries outside the EEA, some of which do not provide equivalent protection for Personal Data.

When transferring your Personal Data to Processors located in countries outside the EEA, we rely on the EU Standard Contractual Clauses or SCCs as a legal basis for transferring and Processing such data.

CCPA

To the extent that we Process any Personal Data relating to individuals who are California residents, we shall comply with the CCPA. For the purposes of the CCPA, you agree that we are a “Service Provider” in the performance of our obligations, and that our customer is a “Business.” As a Service Provider, we shall not: (a) retain, use, or disclose any Personal Data: (i) for any purpose other than for the specific purpose of providing the Seclore Products, including for a commercial purpose other than providing the Seclore Products; (ii) outside of the direct business relationship between us and the customer; or (iii) or as otherwise permitted by the CCPA; or (b) sell Personal Data. Finally, the transfer of the Personal Data to us shall not be considered a “sale” as defined in the CCPA.

YOUR RIGHTS

DATA SUBJECT ACCESS REQUEST:

You have the right to ask us to confirm what Personal Data we hold about you and provide you with a copy of that data.

DATA RECTIFICATION

You have the right to ask us to correct any Personal Data that is inaccurate.

RIGHT TO BE FORGOTTEN

You have the right to ask us to remove your Personal Data where there is no good reason for us to continue to hold that data.

RESTRICTION OF PROCESSING

You have the right to ask us to temporarily stop using your Personal Data if you are questioning our right to use that data and in other circumstances where that right is applicable.

OBJECTION TO PROCESSING

You have the right to ask us to stop using your Personal Data unless we can demonstrate a valid reason why we need to continue to hold that data.

PORTABILITY RIGHT

You have the right to ask us to provide you with the Personal Data that you have provided to us, in a structured and commonly used electronic format, or transmit that information back to you or directly to another company if that is technically feasible.

Our security procedures mean that we may request proof of identity before we are able to disclose your Personal Data to you or comply with other requests.

In some cases, your ability to access or control your Personal Data may be limited by applicable law, contract, or the Product you are using. If you seek to access and control the Personal Data provided to us by your organization, you may contact us at dpo@seclore.com or your organization itself (the Controller).

COOKIES

To personalize your user experience, we may use cookies. A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. We may combine the general information collected through cookies with other Personal Data in connection with our collection of individual usage information. Cookies enhance our Products’ user experience in important ways such as personalizing the user

experience or making the user journey more convenient. Cookies cannot read data from the User's computer's hard disk, read cookie files from other websites, nor from memory of an electronic device. For more information on our use of Cookies, please go through the Seclore Cookie Notice which can be accessed through Seclore License Portal.

SECURITY PROCEDURES:

To protect against the loss, misuse, and alteration of the information under our control, we have in place appropriate physical, electronic, and managerial procedures. For example, our servers are accessible only to authorized personnel and your Personal Data is shared with respective personnel on a need-to-know basis to complete the transaction and to provide the Products.

We follow generally accepted industry standards to protect Personal Data both during transmission and once we receive it. No method of transmission over the internet, or method of electronic storage, however, is 100% secure. Therefore, while we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security. For more information on the technical and organizational security measures adopted by us, refer to Exhibit 1 (Security Measures).

UPDATES TO THIS NOTICE

We may update this Notice from time to time by notifying you of such changes by any reasonable means, including by posting a revised version of this Notice on the Seclore License Portal. Download, access, or use of Seclore Products by you following any changes to this Notice will constitute your acceptance of such changes. The "Last Updated" legend above indicates when this Notice was last changed. We advise you to review this Notice periodically for any changes.

CONTACT US

If you have any enquiries or complaints about how we process your Personal Data, please contact us at: dpo@seclore.com.

DEFINITIONS

- i. **"CCPA"** means California Consumer Privacy Act (as amended), Cal. Civ. Code §§ 1798.100 et seq. including any amendments and implementing regulations that become effective on or after the effective date of this Notice.
- ii. **"Controller"** means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- iii. **"File"** means any document, including without limitation e-mail, protected using Seclore Product.
- iv. **"Identified or Identifiable Natural Person"** means a natural person (individual) who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
- v. **"Personal Data"** means any information relating to an Identified or Identifiable Natural Person and, for the purpose of the Subscription Agreement, this term includes (without limitation) any Personal Data Processed, by Seclore as a result of entering into or performing its obligations under the Subscription Agreement and any associated documents.
- vi. **"Processor"** means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.
- vii. **"Process", "Processed" or "Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- viii. **"Services"** has the meaning ascribed to the term in the Subscription Agreement.
- ix. **"Sub-Processor"** means any third-party engaged by Seclore for Processing Personal Data on behalf of Seclore.
- x. **"User"** means one named individual authorized to use Seclore Products.
- xi. **"Subscription Agreement"** means the agreement executed between Seclore's customer and Seclore for provisioning the Seclore Product.
- xii. **"Subscription Term"** has the meaning ascribed to the term in the Subscription Agreement.
- xiii. Capitalised Terms which are not defined in this Notice have the meaning ascribed to the term in the Subscription Agreement.

EXHIBIT 1

SECURITY MEASURES (INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF DATA)

The purpose of this Notice is to establish guidelines and procedures to ensure the security, protection, auditability, and compliance of all Personal Data collected, Processed, stored, and transmitted by Seclore. This Notice aims to safeguard Personal Data, maintain data integrity, and comply with relevant laws, regulations, and industry standards.

Scope

This policy applies to all employees, contractors, third-party vendors, and any other entities with access to Seclore's data and information systems.

1. Data Handling

- Access to data is granted on a need-to-know basis.
- Encryption mechanisms are employed for data in transit and at rest.
- Employees must follow proper procedures for data disposal.

2. Access Control and Authentication

a. User Access:

- Access rights are assigned based on job responsibilities.
- Quarterly access reviews are conducted to ensure appropriateness.

b. Authentication:

- Strong password policies will be enforced.
- Multi-factor authentication (MFA) is implemented for sensitive systems.

3. Data Security Measures

a. Network Security:

- Networking technology is designed to resist attacks by malicious users or malicious code.
- Web application Firewalls, XDR, intrusion detection systems, anomaly detection systems and other security measures are in place to protect the network infrastructure.

b. Endpoint Security:

- All devices accessing network have up-to-date antivirus software and security patches.

c. Data Encryption:

- Data in transit and data at rest are encrypted using industry-standard algorithms.

4. Audit and Monitoring

a. Logging and Monitoring:

- Logging mechanisms are implemented to record access and activities.
- Regular monitoring is conducted to detect and respond to security incidents.

b. Audit Trails:

- Audit trails are maintained for at least 6 months to track changes to sensitive data and system configurations.

5. Compliance

Seclore will align with the physical, technical, operational, and administrative measures and protocols regarding data security as set forth in its then current SOC 2 Type II Report ("SOC 2"), received from its third-party auditors. Upon written request, Seclore will provide customer with copies of the then-current SOC 2 report issued by its third-party independent auditors in relation to the data security policies and procedures designed to meet the requirements set forth in this Notice.

6. Security Audit

Seclore shall conduct at least annually a Security Audit (VAPT) covering the cloud infrastructure utilized to provide the Software and /or Service and will furnish to the customer the results thereof promptly following customer's written request.

EXHIBIT 2
LIST OF SECLORE ENTITIES

Entity's Legal Name	Principle Place of Business
Seclore Technology Inc (STI)	5201, Great America Parkway, Suite 440, Santa Clara, CA 95054, United States.
Seclore Inc (SI)	5201, Great America Parkway, Suite 440, Santa Clara, CA 95054, United States.
Seclore Technology Private Limited (STPL)	Unit No 1002 and 1004, R Square, 10th Floor, Near J B Nagar Metro Station, Andheri Kurla Road, Bhim Nagar, Andheri East, Mumbai, Maharashtra 400059, India.
Seclore Technologies FZ LLC (Seclore Dubai)	Executive office 107A, DIC Building 10, Dubai Internet City, Dubai, PO BOX NO. 73030, United Arab Emirates.
Seclore GmbH (Seclore Germany)	Inzlingen Geschäftsanschrift: c/o Go-On Group, Fritz-Vomfelde-Straße 6, 40457 Düsseldorf, Germany.
Seclore Technology for Cyber Security Company (Seclore KSA)	Building No.2727, Anas Bin malik Street, Al Sahafah district, Riyadh 13321, Saudi Arabia.