

Secro Landing Web-Page Privacy Policy v. 20250828

This Privacy Policy outlines how Secro Inc. (“we,” “our,” “us”) collects, uses, and discloses Customer information when using our services. It also explains the Customer’s privacy rights and how they are protected by law. By accessing or using our service, the Customer agrees to the collection and use of information in accordance with this Privacy Policy.

1) Interpretation and Definitions

a) Interpretation

Capitalized terms have the following meanings, regardless of singular or plural form.

b) Definitions

i) **Account:** A unique account created for the Customer to access our Service or parts of it.

ii) **Company:**

Secro Inc., 16192 Coastal Hwy, Lewes, DE 19958, United States. For GDPR purposes, the Company is the Data Processor.

iii) **Cookies:** Small files placed on the Customer’s device by a website to track browsing history.

iv) **Country:** United States of America (Delaware).

v) **Customer:**

The individual or legal entity accessing or using the Service. Under GDPR, the Customer is the Data Controller.

vi) **Device:** Any device used to access the Service, including computers and mobile devices.

vii) **Personal Data:** Any data relating to an identifiable individual, as defined under GDPR and the FADP.

viii) **Service:** Refers to Secro Website and Secro Application.

ix) **Sub-Processor:** Third parties who process data on behalf of Secro.

x) **Usage Data:**

Automatically collected data from the Service usage, such as IP addresses, device identifiers, and browsing patterns.

xi) **Website:** Refers to Secro’s landing page and applications available at secro.io.

2) Collection and Use of Customer’s Personal Data

a) Types of Data Collected

i) **Personal Data:**

This includes information such as: name, email address, company name.

If the Customer does not provide necessary information, they may be unable to use certain Service features.

ii) **Usage Data:**

This is automatically collected, including device info, IP addresses, browser details, time logs, diagnostic data, etc.

iii) **Cookies and Tracking Technologies:**

We use cookies for service optimization and tracking. Customers can manage their cookie preferences through the Secro Cookie Consent Manager.

b) **Use of Customer’s Personal Data**

We may use Customer’s data to:

- i) Provide and maintain the Service.
- ii) Manage Customer’s account and process transactions.
- iii) Send updates, promotions, and relevant communications.
- iv) Evaluate and improve our Service and marketing efforts.

v) Transfer data in case of mergers or business reorganization.

c) Retention of Personal Data

We retain Customer data only as long as necessary for the specified purposes and legal obligations. Usage Data may be kept longer for service improvement and security purposes.

d) Transfer of Personal Data

Customer data may be processed in different jurisdictions, including outside their country. By using the Service, the Customer agrees to such data transfers, with all reasonable safeguards in place.

e) Disclosure of Personal Data

We may disclose Personal Data:

- i) In business transactions like mergers or acquisitions.
- ii) To comply with legal requests or prevent fraud.
- iii) With Customer's consent for specific purposes.

f) Security of Personal Data

We implement advanced security measures to protect Customer data, including encryption and secure servers.

3) Detailed Information on Sub-Processors

We may use third-party vendors for services such as cloud hosting, KYC/AML checks, customer support, and analytics. All third-party Sub-Processors comply with GDPR and relevant data protection regulations. List of current sub-processors is available upon written email request to privacy@secro.io.

4) Data Breach Notification

If a data breach occurs, we will notify Customers as soon as practicable and take appropriate measures to limit any data compromise.

5) GDPR Privacy

a) Legal Basis for Processing Personal Data

We may process Personal Data based on:

- i) Customer consent.
- ii) Performance of a contract.
- iii) Legal obligations.
- iv) Legitimate interests.

b) Customer Rights Under GDPR

Customers have the right to:

- i) Access, update, or delete their Personal Data.
- ii) Object to or restrict processing.
- iii) Withdraw consent for processing.
- iv) Request data portability.

Customer may exercise above rights through email privacy@secro.io.

6) FADP Privacy

We comply with the Swiss Federal Act on Data Protection (FADP) and align our practices with GDPR, including data transfer and security protocols.