Secro Privacy Policy

Last updated: November 20th, 2024

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Customer's information when the Customer use the Service and tells the Customer about Customer's privacy rights and how the law protects the Customer.
We use Customer's Personal data to provide and improve the Service. By using the Service, the Customer agrees to the collection and use of information in accordance with this Privacy Policy.

1) Interpretation and Definitions

a) Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

b) Definitions

For the purposes of this Privacy Policy:
Account means a unique account created for the Customer to access our Service or parts of our Service.
Company (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to Secro Inc, 251 Little Falls Drive Wilmington, DE 19808. For the purpose of the GDPR (General Data Protection Regulation), the Company is the Data Processor.
Cookies are small files that are placed on Customer's computer, mobile device or any other device by a website, containing the details of Customer's browsing history on that website among its many uses.
Country refers to: Delaware, United States
Customer means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.
Under GDPR (General Data Protection Regulation), the Customer can be referred to as the Data Controller.
Data Controller, for the purposes of the GDPR, refers to the Customer as the legal person which alone or jointly with others determines the purposes and means of the processing of Personal Data.
Device means any device that can access the Service such as a computer, a cellphone or a digital tablet.
Do Not Track (DNT) is a concept that has been promoted by US regulatory authorities, in particular the U.S. Federal Trade Commission (FTC), for the Internet industry to develop and implement a mechanism for allowing internet users to control the tracking of their online activities across websites.
Personal Data is any information that relates to an identified or identifiable individual.
For the purposes of GDPR, Personal Data means any information relating to the Customer such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
For the purpose of FADP, Personal Data means all information relating to an identified or identifiable person.
Service refers to the Secro Website and Secro Application.
Service Provider means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analyzing how the Service is used. For the purpose of the GDPR, Service Providers are considered Data Sub-Processors.
Usage Data refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).

Website refers to Secro landing page and Secro applications, accessible from https://secro.io, https://sandbox.secro.io, https://platform.secro.io .

2) Collecting and Using Customer's Personal Data

a) Types of Data Collected

i) Personal Data

In order to use Our Service, the Customer might provide Us with certain personally identifiable information. Personally identifiable information may include, but is not limited to:

Email address
First name and last name
Date of birth
State-issued ID numbers
Phone number
Address, State, Province, ZIP/Postal code, City
Usage Data

The Customer has choices about whether he visits our websites, installs our apps, or provides personal information to us. However, if the Customer does not provide us with certain personal information, he may not be able to use some parts of our Services. For example, if he does not provide his legal name and date of birth, then he will not be able to pass KYC and AML checks needed to onboard the Secro platform.

ii) Usage Data

Usage Data is collected automatically when using the Service.

Usage Data may include information such as Customer's Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that the Customer visit, the time and date of Customer's visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When the Customer accesses the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device the Customer use, Customer's mobile device unique ID, the IP address of Customer's mobile device, Customer's mobile operating system, the type of mobile Internet browser the Customer uses, unique device identifiers and other diagnostic data.

We may also collect information that Customer's browser sends whenever the Customer visits our Service or when the Customer accesses the Service by or through a mobile device.

iii) Tracking Technologies and Cookies

Our website https://secro.io uses Cookies to track the activity on Our Service and store certain information. The Customer can choose to decline cookies through the browser settings. However, if the Customer declines cookies, he may not be able to use some parts of our Services. The Customer has the right to decide whether to accept or reject cookies, and can control the cookies preferences from the Secro Cookie Consent Manager available on the Secro website.

b) Use of Customer's Personal Data

The Company may use Personal Data for the following purposes:

To provide and maintain our Service, including to monitor the usage of our Service.

To manage Customer's Account: to manage Customer's registration as a user of the Service. The Personal Data the Customer provides can give the Customer access to different functionalities of the Service that are available to the Customer as a registered user.

For the performance of a contract: the development, compliance and undertaking of the purchase contract for the products, items or services the Customer has purchased or of any other contract with Us through the Service.

To contact the Customer: To contact the Customer by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.

To provide the Customer with news, special offers and general information about other goods, services and events which we offer that are similar to those that the Customer have already purchased or enquired about unless the Customer have opted not to receive such information.

To manage Customer's requests: To attend and manage Customer's requests to Us.

For business transfers: We may use Customer's information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all our assets,

whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.

For other purposes: We may use Customer's information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing and Customer's experience.

We may share Customer's personal information in the following situations:

- **With Service Providers:** We may share Customer's personal information with Service Providers to monitor and analyze the use of our Service, to contact the Customer.
- **With Affiliates:** We may share Customer's information with Our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.
- **With business partners:** We may share Customer's information with Our business partners to offer the Customer certain products, services or promotions.
- **With Customer's consent**: We may disclose Customer's personal information for any other purpose with Customer's consent, such as sharing documents and attachments with other Secro services' users.

c) Retention of Customer's Personal Data

The Company will retain Customer's Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Customer's Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain Customer's data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

d) Transfer of Customer's Personal Data

Customer's information, including Personal Data, is processed at the Company's operating offices, at AWS data centers, and in any other places where the parties involved in the processing are located. It means that this information may be transferred to — and maintained on — computers located outside of Customer's state, province, country or other governmental jurisdiction where the data protection laws may differ than those from Customer's jurisdiction.

Customer's consent to this Privacy Policy followed by Customer's submission of such information represents Customer's agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Customer's data is treated securely and in accordance with this Privacy Policy and no transfer of Customer's Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Customer's data and other personal information.

e) Disclosure of Customer's Personal Data

i) Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Customer's Personal Data may be transferred. We will provide notice before Customer's Personal Data is transferred and becomes subject to a different Privacy Policy.

ii) Law enforcement

Under certain circumstances, the Company may be required to disclose Customer's Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

iii) Other legal requirements

The Company may disclose Customer's Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public
- Protect against legal liability

f) Security of Customer's Personal Data

The security of Customer's Personal Data is important to Us and it is our priority number one. We strive to use state-of-the-art means to protect Customer's Personal Data as per Secro Data Security and Data Residency Policy.

3) Detailed Information on Sub-Processors

The Service Providers We use may have access to Customer's Personal Data. These third-party vendors collect, store, use, sub-process and transfer information about Customer's activity on Our Service in accordance with their Privacy Policies.

a) AML, KYC, KYB checks

We might use ShuftiPro third party service to perform AML, KYC and KYB checks. This provider complies with GDPR and several other regulations. To know more about their Privacy Policy please visit https://shuftipro.com/compliance

b) Cloud hosting

We use Amazon Web Services (AWS) private cloud infrastructure to host the Secro's application and services. AWS complies with the most relevant data protection and security standards including GDPR. To learn more about their Privacy Policy and compliance please visit https://aws.amazon.com/compliance/data-privacy-faq/

c) Customer ticketing and instant chat system

We use Zendesk as a customer resource management tool. Zendesk complies with multiple regulations on data security, including GDPR. To learn more about their Privacy Policy please visit https://www.zendesk.com/trust-center/

d) Customer resource management

We use Pipedrive as an internal tool to store information about our customers. To learn more about their Privacy Policy please visit https://www.pipedrive.com/en/privacy

e) Two factor authentication

We use Twilio as a messaging service to enable two factor authentication of users. To know more about Twilio Privacy Policy please visit https://www.twilio.com/en-us/legal/sub-processors

f) Analytics

The Secro public-facing website https://secro.io uses Google analytics to collect data on visitors. We pass to Google only anonymized IP address data to protect Customer's privacy. For more information about Google Analytics Privacy Policy please visit http://www.google.com/intl/de/analytics/learn/privacy.html

4) Data breach

Should a loss or unauthorized access to the Customer's data occur, We will notify the Customer that a loss or breach of security has occurred, as soon as is practicable and take necessary measures to limit the compromise of data. This would apply to both personal and commercial data processed by Us.

5) GDPR Privacy

a) Legal Basis for Processing Personal Data under GDPR

We may process Personal Data under the following conditions:

- **Consent:** the Customer has given Customer's consent for processing Personal Data for one or more specific purposes.
- **Performance of a contract:** Provision of Personal Data is necessary for the performance of an agreement with the Customer and/or for any pre-contractual obligations thereof.
- **Legal obligations:** Processing Personal Data is necessary for compliance with a legal obligation to which the Company is subject.
- **Vital interests:** Processing Personal Data is necessary in order to protect Customer's vital interests or of another natural person.
- **Public interests:** Processing Personal Data is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Company.
- **Legitimate interests:** Processing Personal Data is necessary for the purposes of the legitimate interests pursued by the Company.

In any case, the Company will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

b) Customer's Rights under the GDPR

The Company undertakes to respect the confidentiality of Customer's Personal Data and to guarantee the Customer can exercise Customer's rights.

The Customer have the right under this Privacy Policy, and by law if the Customer are within the EU, to:

- **Request access to Customer's Personal Data.** The right to access, update or delete the information We have on the Customer. Whenever made possible, the Customer can access, update or request deletion of Customer's Personal Data by writing us at privacy@secro.io. This also enables the Customer to receive a copy of the Personal Data We hold about the Customer.
- **Request correction of the Personal Data that We hold about the Customer.** The Customer has the right to have any incomplete or inaccurate information We hold about the Customer corrected.
- **Object to processing of Customer's Personal Data.** This right exists where We are relying on a legitimate interest as the legal basis for Our processing and there is something about Customer's particular situation, which makes the Customer want to object to our processing of Customer's Personal Data on this ground. The Customer also has the right to object where We are processing Customer's Personal Data for direct marketing purposes.
- **Request erasure of Customer's Personal Data.** The Customer has the right to ask Us to delete or remove Personal Data when there is no good reason for Us to continue processing it. The request is to be sent via email to privacy@secro.io.
- **Request the transfer of Customer's Personal Data.** We will provide the Customer, or a third-party the Customer has chosen, with Customer's Personal Data in a structured, commonly used, machine-readable format. Please note that this right only applies to automated information which the Customer initially provided consent for Us to use or where We used the information to perform a contract with the Customer.
- **Withdraw Customer's consent.** The Customer has the right to withdraw Customer's consent on using Customer's Personal Data. If the Customer withdraws Customer's consent, We may not be able to provide the Customer with access to certain specific functionalities of the Service.

c) Exercising of Customer's GDPR Data Protection Rights

the Customer may exercise Customer's rights of access, rectification, cancellation and opposition by contacting Us. Please note that we may ask the Customer to verify Customer's identity before responding to such requests. If the Customer make a request, We will try our best to respond to the Customer as soon as possible.

The Customer has the right to complain to a Data Protection Authority about Our collection and use of Customer's Personal Data. For more information, if the Customer is in the European Economic Area (EEA), please contact Customer's local data protection authority in the EEA.

6) FADP Privacy

The Swiss Federal Act on Data Protection (FADP) aims to protect the privacy and the fundamental rights of persons when their data is processed. A revised version of the Act is entering into force on September the 1st, 2023, as adopted by the Swiss parliament on September 25th 2020. This update version aligns Swiss requirements for data protection to those of the GDPR. Secro is actively working to comply with the requirement of FADP ahead of its entry into force. As of today Secro is already aligned with the requirements of FADP as far as it:

- Does not transfer any personal data to a third country that is not providing an adequate personal data protection, without the consent of the Customer
- Has a Privacy Policy for its website and application
- Has a Data Protection Officer (Privacy Officer) reachable at privacy@secro.io.
- Is in the process of appointing a Swiss-based Point of Contact person, who will be reachable at privacy@secro.io.