SSG 5001

Data Privacy Policy

segura.security

This Privacy Policy describes the policies and procedures regarding the collection, processing, and storage of your data when you use the Segura Service or Product and reveals how Segura complies with privacy requirements.

Segura collects data, including personal data, to provide and improve our services and products. By using any of our Services or Products, you agree to the collection and use of information in accordance with this policy.

Interpretation

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

Definitions

For the purposes of this Policy

- **You** This refers to the individual accessing or using the Service, or the company or other legal entity accessing or using the Service, as applicable. Under the General Data Protection Regulation, you may be referred to as the Data Subject or the User.
- **Service** refers to the Application or the Website or both provided by the Company.
- **Account** It means a unique account created so that you can access our Service or parts of our Service.
- **Affiliate** means an entity that controls, is controlled by, or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interests, or other securities with voting rights for the election of directors or other administrative authority. 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.
- **Application** This refers to the software program provided by the Company that you have downloaded/activated/accessed on any electronic device.
- **Company**(referred to as "the Company," "We," "Us," or "Our" in this Agreement) in the U.S.: senhasegura USA LLC; in Brazil: MT4 Tecnologia LTDA. For purposes of the CCPA (California Consumer Privacy Act), the Company is defined as the legal entity that collects consumers' personal information and determines the purposes and means of processing consumers' personal information, or on whose behalf such information is collected and which alone, or jointly with others, determines the purposes and means of processing consumers' personal information, and does business in the State of California.
- **Business partner**any person or entity other than the Consumer/You, which includes, but is not limited to, subsidiaries, affiliates, partners, suppliers, or companies resulting from a merger, spin-off, or acquisition.
- **Consumer**For purposes of the CCPA (California Consumer Privacy Act), a resident means an individual who is a resident of California. A resident, as defined by law, includes (1) any individual who is in the U.S. for

purposes other than temporary or transitory purposes and (2) any individual who is domiciled in the U.S. who is outside the U.S. for temporary or transitory purposes, for the purposes of the GDPR.

- **Cookies** These are small files that are placed on your computer, mobile device, or any other device by a website, containing details of your browsing history on that website, among other uses.
- **Country** This refers to the place and originating legislation. Applicability: (1) CCPA: United States; (2) GDPR: European Union; (3) LGPD: Brazil.
- **Data Controller** For the purposes of the GDPR (General Data Protection Regulation) and LGPD (Brazilian General Data Protection Law), "Company" refers to the legal entity that, alone or jointly with others, determines the purposes and means of processing Personal Data.
- **Device** means any device that can access the Service, such as a computer, a mobile phone, a digital tablet, or any other powered device connected to a network.
- **Do Not Track (DNT)**It is a concept that has been promoted by US regulatory authorities, particularly the US Federal Trade Commission (FTC), for the Internet industry to develop and implement a mechanism that allows Internet users to control the tracking of their online activities through websites.
- **Personal data** This includes any information relating to an identified or identifiable individual. Applicability:
    - For the purposes of the GDPR and LGPD, Personal Data means any information relating to you, such as your name, identification number, location data, online identifier or one or more factors specific to your physical, physiological, genetic, mental, economic, cultural or social identity.
    - For the purposes of the CCPA, Personal Data means any information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked to, you, directly or indirectly.
- **Sensitive data** They have specific characteristics depending on each law or regulation. Applicability:
    - A CPRA (California Privacy Rights Act), amendment to CCPA(California Consumer Privacy Act), It considers the following as sensitive personal data: social security number, driver's license number, state identification document or passport; account access credentials (such as login and password); complete financial information (such as bank account number or credit card with security codes); precise geolocation data; racial or ethnic origin, religious or philosophical beliefs and trade union membership; content of private communications (such as emails and messages, when the company is not the recipient); genetic data; biometric data usedfor identification purposes; health-related information; and data about sex life or sexual orientation.
    - The GDPR considers personal data to include: information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed solely for the purpose of identifying a human being; data concerning health; data concerning a person's sex life or sexual orientation.
    - The LGPD (Brazilian General Data Protection Law) considers the following as personal data: Ethnic, political, religious, union or philosophical belief data, health data, sex life or sexual orientation data, genetic and biometric data.

- **Sale**For the purposes of the CPRA, a sale is considered to have occurred when personal data is disclosed, made available, transferred, or communicated to third parties in exchange for financial compensation or other consideration of value.
- **Service provider** This means any natural or legal person who processes 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 purposes of the GDPR, Service Providers are considered Data Processors.
- **Usage data** These refer to data collected automatically, generated by the use of the Service or the Service's own infrastructure.
- **Website** refers to Segura, accessible fromsegura.security or any other domain and subdomain of Segura.

Collection and use of your personal data

We pride ourselves on being an organization with a very strong culture of privacy and security, consistent with legal requirements. We guarantee that your personal data is:

Processed in a legal, fair and transparent manner;

Collected only for clear and legitimate purposes;

Limited in scope and time only to the extent necessary for the purpose of this processing;

Kept accurate and up-to-date;

Protected against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

This privacy policy describes how Segura will process personal data in connection with your use of Segura Services, the website, and other technical applications, tools, or services.

Types of data collected

Personal data

When using our service, we may ask you to provide us with certain personal information that can be used to contact you or identify you. This information may include, but is not limited to:

Email address;

First and last name;

Phone number;

Address, State, Province, Zip Code/Postal Code, City;

Enterprise;

Position or Title;

If you are a Segura customer or business partner, we may also collect additional information such as, for example, login password, biometric information, photos, and payment details.

If you are a candidate to work at Segura or are part of our talent pool for future opportunities,We may also collect and process additional information, as the process progresses through the phases, from the following categories:

Additional identification information, such as: date of birth, parentage, identification document, nationality;

Data on professional, academic, and volunteer background;

Health-related data;

Biometric data, such as: photo, image, and voice recording;

Leisure interests;

Public information from social media/traditional media;

Immigration and work situation, gap activities/travel;

Professional sanctions and inclusion on global blacklists;

Financial and credit data;

Records of judicial, administrative, and criminal proceedings.

This data will be collected considering the minimum necessary for analyzing the suitability of the candidate's profile for the intended position/function, and according to the evaluation phase the candidate is in.

It is essential that you, or a person authorized by you, fill in your personal data with true and up-to-date information. Civil and/or criminal liability for the veracity, accuracy, and authenticity of the data provided in our database rests exclusively with you.

Application

While using our application, to provide its functionalities, we may collect, with your prior permission:

Information about your location

Date and time of access

Your name and email address

Your activity

Our software collects anonymous, non-personal data related to your use of the software ("Usage Data"). This data includes, but is not limited to, technical information such as the type of hardware used, the operating system version, patterns of interaction with the software (e.g., features used most frequently), and application performance metrics.

Tracking Technologies and Cookies

We use cookies and similar tracking technologies to track activity on our Service and store certain information. The technologies we use may include:

Cookies or (literally translated) Browser Cookies: You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept our cookies, you may not be able to use some parts of our Service. Our Service may use cookies. Cookies can be "persistent" cookies or "session" cookies. Persistent cookies remain on your personal computer or mobile device when you go offline, while session cookies are deleted as soon as you close your web browser.

Web Beacons: Some sections of our Service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that allow the Company, for example, to count users who visited those pages or opened an email and for other related statistics.

User behavior: This refers to their behavior on the site, actions, decisions, and choices that people make when interacting with technology and online platforms.

We use both Session and Persistent Cookies for the purposes defined below:

Necessary / Essential Cookies: The type of cookies is Session Cookies. The purpose of these cookies is essential to provide you with our services available through the Website and to allow you to use some of its features. They help authenticate you and prevent fraudulent use of accounts. Without these cookies, the services you have requested cannot be provided, and we only use these cookies to provide you with these services.

Cookie Policy / Cookie Acceptance Notice: The type of persistent cookies and the purpose of these cookies identify whether users have accepted the use of cookies on the website.

Functionality cookies Persistent Cookies: The purpose of these cookies is to allow us to remember the choices you make when using the Website, such as remembering your login details or language preference. The purpose of these cookies is to provide you with a more personal experience and prevent you from having to enter your preferences every time you use the Service.

If you do not accept our cookies, you may experience some inconveniences while using the site and some features may not function correctly.

To avoid using cookies on this website, you will need to take the following steps: disable cookies in your web browser and clear any cookies associated with this website that have been saved in your browser. This option is available to you at any time and will prevent the use of cookies. If you wish to delete cookies or direct your browser to reject or delete them, please consult the help section of your web browser.

Usage

The Company may use Personal Data for the following purposes:

To provide and maintain our Service, including monitoring the use of our Service.

To improve the usability and functionality of our products and services, diagnose technical problems, and optimize software operability.

To train, develop, and improve artificial intelligence algorithms used to enhance Cloud Entitlements and PAM Core software.

To manage your account: to manage your registration as a user of the Service. The Personal Data you provide may give you access to different features of the Service that are available to you as a registered user.

For the performance of a contract: the development, fulfillment and commitment to the purchase agreement for the products, items or services that you have purchased or any other agreement with us through the Service.

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

To provide you with news, special offers, and general information about other goods, services, and events we offer that are similar to those you have already purchased or inquired about, unless you have opted out of receiving such information.

To manage your orders: To process and manage your requests to us.

To deliver targeted advertising to you: We may use your information to develop and display content and advertising (and work with third-party providers who do so) tailored to your interests and/or location and to measure its effectiveness.

For business transfers: We may use your information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of a bankruptcy, liquidation, or similar proceeding, in which Personal Data held by us about users of our services are among the assets transferred.

For recruitment processes: To assess your suitability for available positions, establish contact during the selection process stages, and maintain a talent pool for future opportunities.

For other purposes: We may use your information for other purposes, such as data analysis, preventing or investigating potential security incidents or fraud, identifying usage trends, determining the effectiveness of our promotional campaigns, and evaluating and improving our services, products, marketing, and your experience.

We may share your personal information in the following situations:

With Service Providers: We may share your personal information with Service Providers to monitor and analyze the use of our Service, to advertise to you on third-party websites after you have visited our Service, for payment processing, to conduct research and analysis in recruitment processes for job openings, and to contact you.

For business transfers: We may share or transfer your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or part of our business to another company.

With Affiliates: We may share your information with our affiliates, in which case we 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 your information with our business partners to offer certain products, services, or promotions.

With other users: When you share personal information or otherwise interact in public areas with other users, that information can be seen by all users and may be publicly distributed outside of public areas.

With your consent, We may disclose your personal information for any other purpose with your consent.

Treatment

We will be the controller. We are responsible for the processing of your personal data in our dealings with job applicants and professionals. Similarly, you will be responsible for the processing of your personal data when you enter it through the website.segura.security or other subdomains of segura.security captured by our portfolio. In these cases, it is our responsibility to appropriately choose the legal bases in accordance with the purposes set out in this policy, as well as to respond directly to your requests regarding the rights provided for in current legislation.

We may process Personal Data under the following conditions:

Consent: You have given your consent to the processing of Personal Data for one or more specific purposes.

Performance of a contract: The provision of personal data is necessary for the performance of a contract with you and/or for any pre-contractual obligations thereof.

Legal obligations: The processing of personal data is necessary for compliance with a legal obligation incumbent upon us, as well as for legitimate business purposes authorized by the LGPD, GDPR,CPRA or other applicable regulations.

Vital interests: The processing of personal data is necessary in order to protect your vital interests or those of another natural person.

Public interests: The processing of 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: The processing of Segura usage data is based on our legitimate interest in improving our Software and providing you with an enhanced user experience.

Retention

The company retains your personal data only for as long as necessary for the purposes set out in this Privacy Policy. We retain and use your personal data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. We follow the following parameters to determine the retention period of your personal data:

Time required to fulfill the purpose of the data collection.

When you stop using our website;

Revocation of consent or request for deletion of data by you, only if and when the legal basis for data processing is consent;

Fulfillment of duties and obligations;

Legal deadlines, court decisions, or deadlines determined by the ANPD (National Data Protection Authority);

Deadlines for the controller to comply with legal or regulatory obligations;

Contract execution period;

Period for defense or exercise of rights by "Segura" and licensors;

Transfer to third parties, provided that the processing requirements set out in applicable legislation are met;

For controller use only.

The company also retains 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 improve the functionality of Our Service, or we are legally obligated to retain this data for longer periods of time.

Transfer

Your information, including personal data, is processed at the company's operating offices and anywhere else the parties involved in the processing are located. This means that this information may be transferred to and maintained on computers located outside of your state, province, country, or other governmental jurisdiction where the data protection laws may differ from those of your jurisdiction.

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

Exclusion

You have the right to erase, or request that we help erase, Personal Data associated with you that we have collected about you.

Our Service may give you the option to delete certain information about yourself from within the Service.

You can update, change, or delete your information at any time by accessing your account, if you have one, and visiting the account settings section that allows you to manage your personal information.

You can also contact us to request access to, correct, or delete any personal information you have provided to us. Please note, however, that we may need to retain certain information when we have a legal obligation or legal basis to do so.

Disclosure

Commercial transactions

If the company is involved in a merger, acquisition, or sale of assets, your personal data may be transferred. We will notify you before your Personal Data is transferred and becomes subject to a different Privacy Policy.

Law enforcement

Under certain circumstances, the Company may be required to disclose your personal data if required by law or in response to valid requests from public authorities (for example, a court or government agency).

Other legal requirements

The Company may disclose your personal data in good faith, believing that such action is necessary to:

To comply with a legal obligation;

To protect and defend the rights or property of the Company;

To prevent or investigate potential errors in connection with the Service;

To protect the personal safety of Service Users or the public;

Legal responsibility.

Security of your personal data

The security of your personal data is important to us, but remember that no method of transmission over the Internet or method of electronic storage is 100% secure. To protect personal data in accordance with the requirements and security of our procedures, according to the level of risk and the service provided, we have a team responsible for managing it in accordance with the standards, procedures, or other relevant factors that may influence data protection.

Due to the nature of the Internet, there is a risk that malicious third parties may improperly access information. If this occurs, we are liable within the limits provided by applicable law and may be subject to monetary compensation up to the value of the contract.

The service providers we use may have access to your personal data. These third-party providers collect, store, use, process, and transfer information about your activity on our Service in accordance with their Privacy Policies.

If any intrusion, attempt, or activity is identified that violates or infringes intellectual property rights laws and/or the provisions stipulated in this Policy, terms of use, and/or applicable laws in force, the responsible party will be subject to applicable sanctions, as provided by law or stipulated in this document. The responsible party must also compensate for any damage caused.

Email Marketing

We may use your personal information to contact you with newsletters, marketing or promotional materials, and other information that may be of interest to you. You can opt out of receiving any or all of these communications from us by following the unsubscribe link or instructions provided in any email we send, or by contacting us.

We can use Email Marketing Service Providers to manage and send emails for you.

Payments

We may provide paid products and/or services within the Service. In that case, we may use third-party services for payment processing (e.g., payment processors).

We do not store or collect your payment card details. This information is provided directly to our third-party payment processors whose use of your personal information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS, as administered by the PCI Security Standards Council, which is a joint effort of brands such as Visa, Mastercard, American Express, and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

Credit Card

The available credit card may collect, store, use, process, and transfer information about your activity on Our Service in accordance with its Privacy Policy; please consult your credit card issuer to review their privacy policy.

Selection Process

We cancollectand process the personal data of candidates, regardless of their nationality or place of residence, who participate or express interest in participating in our selection processes. This includes, but is not limited to:

Candidates who apply directly for jobs through the company's website.

Candidates nominated by employees or partners

Candidates contacted through active outreach.

Candidates participating in recruitment processes for positions in Brazil and abroad.

The processing of your personal data is based on the need to carry out preliminary procedures for a possible hiring, as provided for in Article 7, item V of Law No. 13.709 - General Law on the Protection of Personal Data (LGPD). From the moment you become a candidate for a vacancy, a legitimate expectation is established that we may assess your suitability for the position and proceed with the necessary steps for a possible hiring.

During the selection process, we use your data. Our contact information will be used to update you on the progress of your application, schedule interviews and assessments, send preparatory materials when necessary, communicate decisions and next steps, provide feedback on your participation when requested, and clarify any questions that may arise during the process.

We recognize that we don't always have immediately available positions that match your professional profile. Therefore, with your consent, we keep your information in our talent database to identify future opportunities that may be suitable for your profile.

This database allows us to proactively contact you when vacancies arise that match your experience and professional aspirations, participate in special candidate relationship programs, invite you to events and webinars related to career development, and maintain an ongoing relationship that benefits both you and our organization.

It is important to highlight that your continued inclusion in our talent pool is based on your expressed interest, and you may request to be removed at any time.

About Our Service Providers

In the recruitment and selection process, theSegura® uses the InHire platform as its primary applicant tracking system (ATS). In addition, in cases where the process of...*background check*Segura® uses the services of the First Advantage platform. These service providers operate...As personal data operators, we process candidate information exclusively on our behalf and in accordance with our instructions, in compliance with the LGPD (Brazilian General Data Protection Law) and other applicable legislation.

Service providers do not use the data for any purpose of their own, being contractually obligated to:

Process the data only to enable the legitimate purposes of the selection process;

Maintain absolute confidentiality regarding all processed information;

Implement appropriate technical and organizational controls to ensure data integrity and availability;

To meet audits and security compliance requirements.

Sharing with third parties

Segura uses third-party providers to collect, store, operate, and transfer information about your activity on our Service in accordance with the Privacy Policies of those providers. The main purposes of this processing are:

To measure and analyze traffic and browsing activity on our service.

Displaying advertisements for our products and/or services on third-party websites or applications.

To measure and analyze the performance of our advertising campaigns.

We may share information, such as hashed email addresses (if available) or other online identifiers collected on Our Service, with these third-party providers. This allows our third-party providers to recognize and deliver advertisements to you across devices and browsers. To read more about the technologies used by these third-party providers and their cross-device capabilities, please see the Privacy Policy of each provider listed below.

The third-party providers we use are:

Google Ads (AdWords): Google Ads (AdWords) remarketing software. For more information about Google's privacy practices, please visit the page onGoogle Privacy & Terms.

Facebook: Facebook's remarketing service. You can learn more about interest-based advertising at [link to Facebook remarketing service].Facebook by visiting this pageFor more information about Facebook's privacy practices, visit the [link to privacy policy].Facebook Data Policy.

LinkedIn: LinkedIn's remarketing service is used to apply retargeting using the LinkedIn Insight Tag. For more information, visit the [link/page/etc.].LinkedIn Data Policy.

HubSpot: HubSpot's remarketing service may collect data when there is interaction with the Website, product, or service. For more information about your rights, please visit your Privacy Policy.privacy practices.

FreshDesk: Customer support software operated by Fresh Works, Inc. The FreshDesk service may collect information from your device. The information collected by FreshDesk is maintained in accordance with your privacy policy.Privacy Policy.

Some of these third-party providers may use technologies that are not related to cookie-blocking and may not be affected by browser settings that block cookies. Your browser may not allow you to block such technologies. You can use the following third-party tools to opt out of the collection and use of information for the purpose of serving you interest-based advertising:

O opt-out do NAI

EDAAs opt-out

Opt-out to TWO

Google O opt-out da Analytics

O opt-out do Facebook

You can opt out of personalized advertising by enabling privacy features on your mobile device, such as Limit Ad Tracking (iOS) and Opt Out of Ads Personalization (Android). Consult your mobile device's help system for more information.

LGPD Privacy

DPO

The DPO, or Data Protection Officer, as described by the LGPD (Brazilian General Data Protection Law), is the person designated by the data controller and the processor to act as a communication channel between the data controller, the data subjects, and the National Data Protection Authority (ANPD). (LGPD, art. 5º, VIII).

We have a DPO (Data Protection Officer). If you need to contact them to respond to requests, please visit their website directly:segura.security/pt-br/portal-data-privacy.

Rights guaranteed by the LGPD (Brazilian General Data Protection Law)

To confirm the existence of data processing, either in a simplified way or in a clear and complete format.

You can access your data, requesting a legible copy in printed format or through secure and appropriate electronic means.

Correct your information when requesting to edit, correct, or update it.

Limit your data when it is unnecessary, excessive, or processed in violation of the law through anonymization, blocking, or deletion.

Request the portability of your data, through a registration data report that (simplified corporate name) handles with you.

Delete your data, processed based on your consent, except in cases provided for by law.

Revoke your consent, preventing the processing of your data.

To be informed about the possibility of not giving consent and about the consequences of refusal.

To obtain information about the public and private entities with which we share your data.

GDPR Privacy

Your rights under the GDPR

The company is committed to respecting the confidentiality of your personal data and ensuring that you can exercise your rights.

Under this Privacy Policy, and by law if you are within the EU, you have the right to:

Request access to your personal data. You have the right to access, update, or delete the information we hold about you. Whenever possible, you can access, update, or request the deletion of your personal data directly within your account settings section. This also allows you to receive a copy of the Personal Data we hold about you.

Request the correction of the personal data we hold about you. You have the right to have any incomplete or inaccurate information we hold about you corrected.

Objection to the processing of your personal data. This right exists when we rely on a legitimate interest as the legal basis for our processing, and there is something in your particular situation that makes you want to object to our processing of your personal data for this reason. You also have the right to object to where we are processing your personal data for direct marketing purposes.

Request the deletion of your personal data. You have the right to ask us to erase or remove your personal data when it is no longer necessary for providing services to you.

Request the transfer of your personal data. We will provide you, or a third party you have chosen, with your Personal Data in a structured, commonly used, machine-readable format. Please note that this right applies only to automated information that you initially consented to us using or where we used the information to perform a contract with you.

Withdraw your consent. You have the right to withdraw your consent to the use of your personal data. If you withdraw your consent, we may not be able to provide you with access to certain specific features of the Service.

Request restriction of processing. You can request that we stop processing all or some of your personal data.

In accordance with legal provisions, we provide access to requests through the website:segura.security/pt-br/portal-data-privacy. For more information, read the topic "Our Responsibility".

CPRA Privacy

Your rights under the CPRA

The California Privacy Rights Act (CPRA) grants California residents specific rights regarding their personal information and sensitive personal information.

If you are a resident of California, you have the following rights:

Right to Notice

You have the right to be informed about:

- As Categories of personal information and sensitive personal informationthat we collect;
- As purposesf or what purposes this information is used;
- Your retention criteriaor the period for which the information will be stored.

Right to Request (Right of Access)

You have the right to request that we disclose information related to ourcollection, use, sale, sharing, and disclosure of personal information. After we receive and confirm your verifiable request, we will disclose:

- The categories of personal information collected about you;
- The categories of sources of personal information;
- Commercial or business purposes for collecting, selling, or sharing;
- The categories of third parties with whom we share personal information;
- Specific personal information is collected about you.

Right to Opt Out of Sale and Sharing

You have the right toopt out of allowing the sale or sharingyour personal information.

To exercise this right, you can contact us through the channels indicated in this policy.

Right to Limit the Use of Sensitive Personal Information

You have the right toLimit the use and disclosure of your Sensitive Personal Information. Only what is strictly necessary for:

- To provide the requested services;
- To fulfill legal obligations;
- To guarantee security and prevent fraud.

Right to Opt Out

You have the right to request the deletion of your personal information, subject to legal exceptions.

After order confirmation, we will delete your personal information from our records and instruct our service providers to do the same, except where retention is necessary to:

- To complete transactions or provide requested services;
- Detect security incidents and prevent fraud;
- Debug and correct errors;
- Exercising freedom of expression or fulfilling legal rights;
- Compliance with legal obligations;
- Scientific, historical, or statistical research of public interest, when applicable;
- Internal uses are consistent with the context in which the information was provided.

Right to Non-Discrimination

You have the right not to be discriminated against for exercising any right provided for in the CPRA, including:

- Denial of goods or services;
- Charging different prices or fees;
- Offering a lower level or quality of services;
- Suggestion for differentiated treatment.

In accordance with legal provisions, we provide access to requests through the website:segura.security/pt-br/portal-data-privacy. For more information, read the topic "Our Responsibility".

Sale of personal information

According to the CPRA, "selling" means disclosing, making available, transferring, or communicating personal information to third parties in exchange for financial consideration or other benefit of value.

The CPRA also defines "sharing" as the disclosure of personal information for behavioral advertising purposes across contexts, even without payment involved.

Segura does not sell or share personal information for behavioral advertising purposes. Information may be shared with partners and service providers strictly for the provision and improvement of our services, always based on applicable legal grounds and, when required, with the consent of the data subject.

Do not sell my personal information.

You have the right to opt out of the sale of your personal information. Once we receive and confirm a verifiable consumer request, we will stop selling your personal information. To exercise your right to opt out, please contact us.

The Service Providers we partner with (for example, our analytics or advertising partners) may use technology in the Service that sells personal information. If you wish to opt out of the use of your personal information for interest-based advertising and such potential sales, as defined by CPRA law, you may do so by following the instructions below.

Please note that any opt-out option is specific to the browser you are using. You may need to opt out of all browsers you use.

Website

You can choose not to receive ads that are personalized as served by our Service Providers by following the instructions provided in the Service:

A plataforma opt-out do NAI: http://www.networkadvertising.org/choices/

A platform has opted-out of the EDAA http://www.youronlinechoices.com/

A platform DAA opt-out: http://optout.aboutads.info/?c=2&lang=EN

Opting out will place a cookie on your computer that is unique to the browser you use to opt out. If you switch browsers or delete the cookies saved by your browser, you will need to opt out again.

Mobile devices

Your mobile device may give you the option to not use information about the apps you use to deliver ads that are targeted to your interests:

"Opt out of Interest-Based Ads" ou "Opt out of Ads Personalization" em dispositivos Android

"Limit Ad Tracking" on iOS devices

You can also stop your mobile device from collecting location information by changing the preferences on your mobile device.

Privacy rights for underage users

Our services are designed for users who are 16 or 18 years of age or older, depending on applicable law. We do not sell the personal information of our customers who are minors unless we receive affirmative authorization (the "opt-in right"). Consumers who opt out of the sale of their personal information may opt out of future sales at any time by sending us a request.

Furthermore, we do not intentionally collect personal information from individuals under the age of 18 or 16, depending on the jurisdiction, through our service. However, we recognize that certain third-party websites to which we provide links may collect and sell personal information from minors. We encourage parents and legal guardians to monitor their children's internet use and instruct their children never to provide information on other websites without their permission.

If you are a California resident under the age of 18 and a registered user of our website, service, or online application, you may request and obtain the removal of content or information that you have publicly posted. To request the removal of such data, please contact us using the contact information provided below. However, please be aware that your request does not guarantee the complete or comprehensive removal of the content or information posted online, and the law may not permit or require removal in certain circumstances.

"Do Not Track" policy as required by the California Online Privacy Protection Act (Cal OPPA)

Our service does not respond to Do Not Track signals.

However, some third-party websites keep track of your browsing activity. If you are visiting such websites, you can set your browser preferences to inform the websites that you do not want to be tracked. You can enable or disable DNT by visiting your web browser's preferences or settings page.

Your privacy rights in California (California's Shine the Light law)

According to Section 1798 of the California Civil Code (California's Shine the Light Law), California residents with an established business relationship with us may request information once a year regarding the sharing of their personal data with third parties for those third parties' direct marketing purposes.

If you would like to request more information about the California Shine the Light law, and if you are a California resident, you can contact us using the contact information provided below in the "Our Responsibility" section.

Links to other websites

Our Service may contain links to other websites that are not operated by us. If you click on a third-party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over, and assume no responsibility for, the content, privacy policies, or practices of any third-party websites or services.

Our responsibility

Honor requests and fulfill them in simple and direct language.

Compliance with the deadline to respond to any request within 45 calendar days. The deadline may be extended for a further 45 days, with notification to the data subject.

Provide "mandatory notices" before collecting information, covering the categories and purposes of personal information.

Provide privacy policies, including information about consumers' privacy rights and how to exercise them: right to know, right to opt out, and right to non-discrimination.

Enable and periodically verify security methods to protect personal and/or sensitive data.

Report any violations to the relevant authorities and the person in question as quickly as possible.

In accordance with legal provisions, we provide access to requests through the website:

segura.security/pt-br/portal-data-privacy.

You have the right to complain to a Data Protection Authority about our collection and use of your personal data.

If you request this from us, you must:

Provide sufficient information to allow us to reasonably verify that you are the person about whom we collect personal information or an authorized representative.

Describe your request in sufficient detail to allow us to understand, evaluate, and respond appropriately.

We cannot respond to your request or provide you with the necessary information if we cannot:

Verify your identity or authority to make the request.

And confirm that the personal information pertains to you.

Changes to this Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will notify you via email and/or a prominent notice on Our Service before the change becomes effective and update the "Updated" date at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Contact us

If you have any questions about this Policy, you can contact us through:

Through our website: segura.security

Email: sales@segura.security | support@segura.security | compliance@segura.security

By phone: +55 11 3069-3925