

PRIVACY POLICY

- *Last Modified: December 27, 2024* -





Preamble

- (1) At SENS LTD (“we,” “our,” or “us”), we are committed to protecting your privacy and ensuring the security of your personal data. This Privacy Policy explains how we collect, use, store, and protect your information when you access or use the SENS Platform (“Platform”).
- (2) We recognize the importance of data privacy and compliance with applicable data protection laws. Our goal is to provide a transparent framework that outlines your rights and responsibilities in relation to your personal information.
- (3) This Privacy Policy applies to: (i.) Users and Authors who register accounts, upload content, or interact with Platform’s features; (ii.) Visitors who browse or access Platform without registering an account; (iii.) Third parties who provide services through Platform or act as integrated payment providers.
- (4) We process your data to: (i.) Enable Platform functionality and deliver services; (ii.) Facilitate secure transactions and verify identities (including KYC); (iii.) Prevent fraud, abuse, and violations of our Terms (iv.) Improve user experience and personalize Platform features. (v.) Comply with legal and regulatory obligations.
- (5) By accessing or using Platform, you consent to the practices described in this Privacy Policy. If you disagree with any part of this Privacy Policy, you must stop using Platform immediately.
- (6) We may update this Privacy Policy from time to time to reflect legal requirements or business changes. We encourage you to review this document regularly to stay informed about how we protect your privacy
- (7) This Policy forms an integral part of our Terms of Service located at <https://sens.love/> and must be read in conjunction with it.
- (8) For questions or concerns regarding this Privacy Policy, please contact us at official@sens.love.



CONTENTS

Article §1: Definitions	4
Article §2: General Provisions	5
Article §3: Your Personal Data Rights and Controls	6
Article §4: Data Processed.....	7
Article §4: Purpose For Using Your Personal Data	8
Article §5: Disclosing Your Personal Data	11
Article §6: Data Retention	12
Article §7: Transfer to Other Countries	13
Article §9: Third-Party Service Providers.....	14
Article §10: Cookies.....	14
Article §11: Storage of Personal Data.....	15
SCHEDULE 1: California Notice at Collection.....	17
SCHEDULE 2: GDPR COMPLIANCE NOTICE	22

Article §1: Definitions

1. **Controller** or **Data Controller** refers to the Company, which determines the purposes and means of processing Personal Data.
2. **Processor** refers to any natural or legal person that processes Personal Data on behalf of the Company under a contractual agreement.
3. **Data Subject** or **User** refers to any natural person who visits the Website and/or uses the Services provided by the Company.
4. **Personal Data** refers to any information that relates to and identifies a Data Subject, either directly or indirectly, including but not limited to name, email address, IP address, and device information. For further details, see the “DATA PROCESSED” Section of this Notice.
5. **Cookies** refers to small fragments of data sent by our web server and stored on a user's device. Cookies enable Website functionality, save user preferences (e.g., language settings), and analyze Website traffic.
6. **Party** refers to either the User (you) or the Company. For the avoidance of doubt, the contracting Parties under this Notice are the User and the Company.
7. **Services** refers to the services provided by the Company via the Website or any associated platforms, including APIs, third-party tools, and marketing communications.
8. **Relevant Legislation** refers to the legal frameworks listed in “GENERAL PROVISIONS” Clause of this Notice, including but not limited to GDPR, CCPA, CPRA, and other applicable laws based on the User's place of residence. Relevant legislation applies according to the jurisdiction where the User resides.
9. **Standard Contractual Clauses (SCCs)** refers to EU-approved model clauses used to ensure the lawful transfer of Personal Data to countries outside the European Economic Area (EEA).
10. **Sensitive Personal Data** refers to categories of Personal Data requiring higher protection under relevant legislation, including data related to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, genetic or biometric data, and sexual orientation.
11. **Supervisory Authority** refers to an independent public authority established under GDPR or other relevant legislation responsible for monitoring and enforcing compliance with data protection laws.
12. **Third-Party Service Providers** refers to external entities contracted by the Company to perform specific functions, such as hosting, payment processing, marketing, analytics, or customer support, that involve the processing of Personal Data.
13. **Anonymization** refers to the process of irreversibly altering Personal Data so that an individual cannot be identified, either directly or indirectly.
14. **Pseudonymization** refers to the processing of Personal Data in such a way that it can no longer be attributed to a specific Data Subject without the use of additional information, which is kept separately and protected by appropriate measures.



- 15. **Consent** refers to the freely given, specific, informed, and unambiguous indication of a Data Subject's wishes by which they signify agreement to the processing of their Personal Data.
- 16. **Profiling** refers to any form of automated processing of Personal Data to evaluate certain personal aspects, such as analyzing or predicting a Data Subject's preferences, behavior, or location.
- 17. **Breach of Personal Data** refers to a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Article §2: General Provisions

- 1. **As** the Data Controller, the Company determines the purposes and means of processing your Personal Data and is responsible for ensuring compliance with Relevant Legislation:

APPLICABLE LEGISLATION	CATEGORY OF USER
The California Consumer Privacy Act of 2018 ("CCPA")	Applies to users located in state of California
the Virginia Consumer Data Protection Act ("VCDPA")	Applies to users located in state of Virginia
the New York SHIELD Act	Applies to users located in state of New York
General Data Protection Regulation (EU Regulation 2016/679, "GDPR")	Applies within the European Economic Area (EEA)

- 2. The application of specific data protection laws depends on the location of the User. For example, GDPR applies to users located within the European Economic Area (EEA), while CCPA, VCDPA, and SHIELD Act apply to users located in California, Virginia, and New York, respectively. The Company ensures that its processing activities comply with the applicable legal requirements based on the user's location.
- 3. This Notice is governed by the principles and requirements set forth in GDPR, CCPA, VCDPA, SHIELD Act, and other relevant laws, ensuring a comprehensive and lawful approach to the processing of Personal Data. The Company adheres to the highest standards of data protection and complies with specific obligations under each applicable law, including honoring consumer rights, ensuring data security, and providing appropriate legal safeguards.
- 4. The Company is committed to:
 - (a) Ensuring transparency and accountability in its data processing activities.
 - (b) Implementing appropriate technical and organizational measures to safeguard Personal Data.

Find Us at <https://sens.love/>

© 2025 Sens (18+). All Rights Reserved



- (c) Processing Personal Data lawfully, fairly, and in a manner that is transparent to Data Subjects.
 - (d) Ensuring that third parties, including Processors, engaged in data processing on behalf of the Company, comply with applicable data protection laws and contractual obligations.
5. The Company also ensures that Data Subjects’ rights under relevant legislation, and other applicable laws—including the right to access, rectify, erase, or restrict the processing of their Personal Data—are respected and enforceable.
 6. If you are a resident of California, the provisions outlined in Schedule 1: California Notice at Collection apply to you in addition to this Privacy Notice. These provisions detail your rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), including specific categories of data collected, purposes of processing, and your right to opt out of certain data-sharing practices.
 7. If you are a resident of the European Economic Area (EEA), the provisions outlined in Schedule 2: GDPR Compliance Notice apply to you in addition to this Privacy Notice. These provisions explain your rights under the General Data Protection Regulation (GDPR), the legal bases for data processing, and safeguards for international data transfers.

Article §3: Your Personal Data Rights and Controls

1. As a Data Subject, you have specific rights regarding your Personal Data under relevant legislation. The Company is committed to ensuring that you can exercise these rights effectively and transparently. Below, we outline your key rights:

ACTION	DESCRIPTION
Right to Access	You have the right to request access to the Personal Data we hold about you, including information about how we process your data, the categories of data processed, and the purposes for processing.
Right to Rectification	You can request that we correct or update inaccurate or incomplete Personal Data about you.
Right to Restrict Processing	You can request that we temporarily or permanently restrict the processing of your Personal Data under specific conditions
Right to Data Portability	You can request to receive a copy of your Personal Data in a structured, commonly used, and machine-readable format, and, where feasible, request that we transfer this data to another controller
Right to Object	You may object to the processing of your Personal Data when it is based on our legitimate interests, public interest, or direct marketing purposes.

Find Us at <https://sens.love/>

© 2025 Sens (18+). All Rights Reserved



Right to Withdraw Consent	Where we rely on your consent to process your Personal Data, you can withdraw this consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.
Right to Lodge a Complaint	If you believe we have violated your data protection rights, you have the right to file a complaint with a supervisory authority in your jurisdiction under the relevant legislation

2. How to Exercise Your Rights? You can exercise your rights by contacting us at official@sens.love. We will review and respond to your request in accordance with relevant legislation and within the required timeframes. To ensure the security of your data, we may need to verify your identity before processing your request.
3. Limitations and Exceptions. Please note that some rights may be subject to limitations under relevant legislation. For example, we may retain certain Personal Data to comply with legal obligations or resolve disputes.
4. To verify a request to access, delete, or correct your data, we may ask you to provide specific details associated with your account. If you do not have an account, we may not possess sufficient information to verify your identity or link your request to prior interactions with our services, as we do not retain data necessary for re-identification. In such cases, we will be unable to fulfill your request.
5. You may authorize an agent to make requests on your behalf by providing written authorization or a valid power of attorney, in accordance with local laws. Before processing such requests, the agent must provide proof of authorization, and we may require direct verification of your identity to ensure the validity of the request.
6. If your request is denied, you may have the right to appeal the decision.

Article §4: Data Processed

1. We rely on the following legal grounds:
 - (a) Your explicit consent with the Policy: We obtain your consent to processing of personal data in accordance with the Policy through consent forms within the Services.
 - (b) Our contractual obligations with Users: We need to collect data in order for us to fulfill Our obligations under the contract concluded between you and us.
 - (c) Our legitimate interest: We need to provide the best and comfortable Services to you as described in our Terms of Service
2. We process the following types of data:

Find Us at <https://sens.love/>

© 2025 Sens (18+). All Rights Reserved



CATEGORY OF DATA	PURPOSE	DESCRIPTION
Registration information (email address, username, and password)	To create and manage your account and provide access to the Services.	1) Contractual necessity; 2) Legitimate interests
Identification information (first and last name, username, address, and phone number)	To confirm your identity and provide personalized services.	1) Legal obligation; 2) Legitimate interests
Commercial information (products browsed, services used, subscriptions)	To personalize your experience and improve our services based on your preferences and activity history.	Legitimate interests
Third-party credentials (passwords, usernames, account numbers for third-party services)	To facilitate integration with Third-Party Services (e.g., payment processors like Stripe, social media platforms).	1) Consent; 2) Contractual necessity
Information from Third-Party Services (account and personal data)	To display information from Third-Party Services you connect under your account.	1) Consent; 2) Contractual necessity
Technical and navigational information (browser, pages visited, time spent, IP address, device ID, operating system version, app version)	To optimize Website performance, ensure security, and improve user experience.	Legitimate interests
Location information (collected from your device)	To provide location-enabled services, if enabled by you.	Consent
Social media information (contact details, aggregate analytics)	To interact with users on Social Media Pages and analyze engagement trends.	1) Consent; 2) Legitimate interests
Email open/click information (email address, IP address, time of interaction)	To analyze the effectiveness of email campaigns and improve communication.	1) Consent; 2) Legitimate interests
KYC Data – Identification Documents (passport, driver’s license, ID)	To verify identity and confirm age in compliance with KYC requirements and prevent underage usage.	1) Legal obligation; 2) Legitimate interests
KYC Data – Biographical Information (name, gender, age, profile bio)	To verify identity, detect fraud, and maintain a safe Platform environment.	1) Legal obligation; 2) Legitimate interests
KYC Data – Profile Data (nickname, profile photo)	To create identifiable profiles for Authors and ensure compliance with Platform rules.	1) Consent; 2) Contractual necessity
KYC Data – Contact Information (email address, phone number)	To provide notifications, ensure secure communication, and verify user accounts.	1) Legal obligation; 2) Contractual necessity
Other information (feedback, questions, suggestions)	To improve the Services and respond to your inquiries.	Consent

Article §4: Purpose For Using Your Personal Data

Find Us at <https://sens.love/>

© 2025 Sens (18+). All Rights Reserved



1. We use your Personal Data for the following purposes, in compliance with relevant legislation:

CATEGORY OF DATA	PURPOSE	DESCRIPTION
Name, e-mail, login, password, phone number. Technical data (e.g., IP address, language, browser type, operating system)	Providing and Managing Our Services as well as with the functionality of the Website	<ol style="list-style-type: none"> 1) To create and manage your account. 2) To enable you to access and use our Website and services. 3) To respond to your inquiries, requests, and technical support needs.
Technical data (e.g., IP address, browser type, country). Usage data (e.g., URL clickstreams, page response times, download errors, time spent on web pages).	Improving and Optimizing Our Services and Website	<ol style="list-style-type: none"> 1) To analyse and improve the functionality and performance of our Website and services. 2) To conduct research and statistical analysis for product development and enhancement. 3) To customize your experience by remembering your preferences, such as language settings.
Name, e-mail, phone number. Usage data (e.g., actions on pages, interactions with content).	Communicating with You	<ol style="list-style-type: none"> 1) To send you service-related communications, such as updates, technical notices, and security alerts. 2) To provide newsletters, offers, and marketing communications (with your consent, where required).
Technical data (e.g., IP address, operating system). Data required for compliance with legislation (e.g., incorporation documents, licenses).	Ensuring Security and Compliance	<ol style="list-style-type: none"> 1) To detect and prevent fraud, unauthorized access, or other illegal activities. <p>To comply with applicable laws, regulatory requirements, and contractual obligations.</p>
Name, e-mail, phone number. Usage data (e.g., browsing behavior, interactions with ads). Technical data (e.g., device type, IP address).	Advertising and Marketing	<ol style="list-style-type: none"> 1) To send newsletters, marketing emails, and updates about our services or offers (with your consent, where required). 2) To deliver tailored advertisements and promotional content based on your activity and preferences (with your consent, where required). 3) To analyze the effectiveness of our marketing campaigns. 4) To subscribe to Our Newsletters/Marketing E-mails/Updates
Identity Data (Full name; Contact details (e.g., email address, phone number, physical address)); Technical Data (IP address; Device and browser information; Logs of interactions with the Website or services); Usage Data (Activity logs (e.g., login times, actions on the Website); Historical records of interactions with the Company (e.g., customer support chats, submitted inquiries);	Legal Obligations and Dispute Resolution.	<ol style="list-style-type: none"> 1) To fulfill legal obligations, such as record-keeping and compliance with government regulations. 2) To comply with a request from law enforcement, courts, or other competent authorities.



PRIVACY POLICY

Last Modified: **DECEMBER 27, 2024**

Dispute Resolution Data (Correspondence with legal representatives or regulatory authorities; Records of prior complaints or disputes; Supporting evidence provided during disputes (e.g., screenshots, emails, contracts); Sensitive Data (ONLY where legally required) (Information related to legal claims or litigation (e.g., case details, legal arguments, court orders).		
Name, e-mail, login, password Usage data (e.g., service interaction logs).	Sharing Personal Data with Authorized Third Parties	To share your Personal Data with authorized third-party service providers and partners to deliver our services effectively (e.g., payment processors, hosting providers, marketing platforms).
Technical data (e.g., IP address, browser type, operating system). Usage data (e.g., suspicious activity logs, interactions with services). Name and contact details (for verification purposes).	Fraud Detection and Prevention.	To detect, prevent, and investigate fraud, unauthorized access, and other illegal activities.
Usage data (e.g., page response times, clickstreams, time spent on pages). Technical data (e.g., device information, operating system).	Performance Monitoring and Analytics	To monitor the performance of our Website and services, gather insights into user behavior, and improve service functionality.
Identity Data (Full name; Contact details (e.g., email address, phone number, physical address)) Transaction Data (Payment details (e.g., payment method, billing information); Transaction history (e.g., dates, amounts, and descriptions of services or products provided)) Technical Data (IP address; Device information; Logs of access and interactions with the services) Usage Data (Activity logs related to the use of services (e.g., API requests, subscription management); Information required for service optimization and analytics shared with partners) Compliance Data (Any required certifications, licenses, or compliance documents necessary for fulfilling legal or contractual obligations)	Fulfilment of Contractual Obligations with Third Parties	To meet the requirements of agreements with third-party service providers, partners, or contractors necessary for the operation and delivery of our services. This includes ensuring proper service integration, reporting, and compliance with contractual terms.
KYC Data – Identification Documents (passport, driver’s license, ID)	Identity Verification and Compliance	1) To verify identity and confirm age in compliance with KYC requirements . 2) To meet legal and regulatory obligations , including anti-money laundering (AML) checks.
KYC Data – Biographical Information (name, gender, age, profile bio)	Fraud Prevention and Platform Security	1) To verify identity, detect fraud, and ensure Platform security. 2) To maintain a safe environment by identifying Authors and Users.
KYC Data – Profile Data (nickname, profile photo)	Profile Creation and Verification	1) To enable Authors to establish profiles and promote their content.

Find Us at <https://sens.love/>

© 2025 Sens (18+). All Rights Reserved



		2) To verify profile authenticity and compliance with Platform rules.
KYC Data – Contact Information (e-mail address, phone number)	Account Security and Communication	1) To provide notifications, updates, and account-related alerts. 2) To verify and recover accounts in case of security breaches.

Article §5: Disclosing Your Personal Data

1. We share your Personal Data with authorized third parties when it is necessary to deliver our services, comply with legal obligations, or meet our legitimate interests. Below are the categories of recipients and the reasons for sharing your Personal Data:

(a) SERVICE PROVIDERS AND PARTNERS

We disclose your Personal Data to trusted service providers and partners who assist us in delivering our services, such as hosting providers, payment processors, marketing platforms, customer support tools, and analytics services. These third parties process your data only under our instructions and in compliance with applicable laws.

- (i) We may share your Personal data with our third party service providers indicated below:
- (ii) website analytics companies to analyze data and improve our services and the Website such as **Google Analytics**;
- (iii) advertising companies for marketing purposes such as **Google AdWords**;
- (iv) social media companies to promote and be present in social media such as **Facebook, Instagram, LinkedIn, Twitter, YouTube, Telegram, GitHub, Discord, medium, Reddit.**

(b) THIRD PARTIES REQUIRED FOR SERVICE INTEGRATION

Certain features of our services rely on integrations with third-party platforms or tools. In such cases, we share relevant Personal Data necessary to enable these integrations, such as technical data and usage logs.

(c) LEGAL AND REGULATORY AUTHORITIES

We may disclose your Personal Data when required to comply with applicable laws, regulations, legal processes, or enforceable governmental requests. This includes providing data to regulatory authorities, courts, or law enforcement to ensure compliance with legal obligations or protect against fraudulent or illegal activities.

(d) BUSINESS TRANSFERS



In the event of a merger, acquisition, or sale of assets, your Personal Data may be shared with the relevant parties involved in the transaction. We will ensure that these parties are obligated to protect your data in accordance with this Privacy Notice and applicable laws.

(e) ADVERTISING AND MARKETING PARTNERS

With your consent, we may share data with advertising partners to deliver personalized advertisements and measure the effectiveness of marketing campaigns. This may include technical data, usage data, and preferences collected through cookies or similar technologies.

(f) DISPUTE RESOLUTION AND LEGAL CLAIMS

We may share your Personal Data with legal representatives, advisors, or other relevant third parties in the context of resolving disputes, enforcing our agreements, or protecting our legal rights.

(g) CONSENT-BASED SHARING

If you explicitly consent, we may share your Personal Data with other third parties for purposes not covered above. You will have the right to withdraw such consent at any time.

2. We ensure that all third parties with whom we share your Personal Data are bound by confidentiality and data protection obligations consistent with applicable laws, including GDPR and other relevant legislation. While we take reasonable steps to verify that these third parties implement adequate safeguards to protect your data, we are not obligated to conduct exhaustive checks and disclaim any liability for breaches, misuse, or non-compliance on the part of these third parties. Your data will never be sold to unauthorized third parties.

Article §6: Data Retention

1. We retain your Personal Data **ONLY** for as long as necessary to fulfill the purposes for which it was collected, as outlined in this Privacy Notice, and to comply with our legal, regulatory, contractual, or legitimate business obligations. Retention periods vary depending on the type of data, the purpose of its processing, and applicable laws.
2. **Account and Service-Related Data:** Personal Data associated with your account, such as your name, email, and login credentials, is retained for as long as your account remains active. If you deactivate your account or cease using our services, we retain this data for a reasonable period to facilitate account recovery, fulfill legal obligations, or address potential disputes.
3. **Technical and Usage Data:** Technical and usage data, such as IP addresses, browser information, and activity logs, is retained for shorter durations unless required for security monitoring, fraud prevention, or legal compliance. Data used for analytics and service optimization may be anonymized and retained for longer periods to improve our offerings.

4. **Legal and Compliance Data:** Data required for compliance with legal obligations, regulatory reporting, or legal claims is retained for as long as mandated by applicable laws or until the resolution of the matter. For instance, documents related to contractual disputes or litigation may be retained for the duration of the statutory limitation periods, which vary by jurisdiction.
5. **Marketing and Communication Data:** Personal Data used for marketing, such as email addresses or preferences, is retained until you withdraw your consent or opt out. After opting out, we may retain minimal information (e.g., email address) to ensure your preferences are respected and to prevent future communications.
6. **Backup and Archival Data:** Data stored in backups for disaster recovery purposes is retained for a limited period according to our internal data retention policy. These backups are securely encrypted and used solely for restoring critical systems in case of emergencies.

Article §7: Transfer to Other Countries

1. Due to the global nature of our business, we may transfer your Personal Data to other countries, including those outside your country of residence, to facilitate our operations and provide services. This may involve sharing Personal Data with our group companies, subcontractors, and trusted partners as described in this Privacy Notice.
2. Whenever we transfer Personal Data internationally, we take reasonable steps to ensure that such transfers comply with applicable laws. This includes efforts to verify that the recipient country or organization offers an adequate level of data protection or implementing additional safeguards where necessary. While we strive to ensure the security and compliance of all data transfers, we are not liable for breaches, misuse, or non-compliance by third parties after taking reasonable and proportionate measures to safeguard your data.
3. We employ various measures to ensure that your Personal Data remains protected during international transfers. These safeguards may include:
 - (a) **Standard Contractual Clauses:** Ensuring data transfers to countries outside the country of residence are governed by approved clauses.
 - (b) **Technical Protections:** Using encryption, pseudonymization, and secure transmission protocols to safeguard your data during transfer and storage.
 - (c) **Policies and Processes:** Implementing strict internal policies to challenge disproportionate or unlawful government requests for access to Personal Data.
 - (d) **Binding Corporate Rules:** Applying intra-group data transfer agreements to maintain consistent data protection standards across our organization.
4. Depending on the nature and destination of the data transfer, we may use additional measures to enhance security and compliance, including:

- (a) Limiting data transfers to the minimum necessary for the purpose.
- (b) Employing dedicated teams to assess and manage risks associated with international data transfers.

Article §9: Third-Party Service Providers

1. Sometimes we may need to share your data with a third party. We may share your data with our contractors provided these third parties assume confidentiality obligations regarding your personal data. Please, be informed that we may disclose your personal data to the following third parties:
 - (a) our group entities or subsidiaries;
 - (b) government or law enforcement officials, enforcement, exchange body, central or local government department and other statutory or public bodies or court;
 - (c) business partners, suppliers, contractors, sponsors, analytics, search engine providers.
2. We may share your personal information:
 - (a) In order to provide our Services to you or to administer them;
 - (b) In order to comply with any applicable laws or regulations. This includes exchanging information for the purposes of detecting and investigating fraudulent or unlawful activity and respond to claims and legal process;
 - (c) To prevent or stop activity we may consider to be, or to pose a risk of being, illegal, unethical or legally actionable or that poses a threat to the safety of you, another person or the public generally;
 - (d) In case of merger, acquisition or any other reorganizations of our company, transfer of control with transfer of all information to the relevant third party with your consent to do so if required by law.
3. Anonymous or aggregated information or other data that does not directly identify you is shared for the analysis. If you would like to get a full list of all third parties with whom we share your data, please, e-mail as the list may vary depending on your specific use of our Services.

Article §10: Cookies

1. Cookies are used when users are logged in, so that the service provider can remember and identify you as users. This prevents you from having to log in every single time you visit a new page. These cookies are typically removed or cleared when you log out to ensure that you can only access restricted features and areas when logged in.

2. When you submit data through a form such as a contact page or comment box, cookies may be set to remember your user details for future correspondence.
3. Some of the cookies used are persistent, which means that they remain stored on your device for one year.
4. In some cases, service providers may provide you with custom content based on what you tell them about yourself, either directly or indirectly if you link a social media account. These types of cookies simply allow these service providers to provide you with content that they feel may be of interest to you.
5. Company uses the following types of cookies:
 - (a) Necessary cookies: help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies. These cookies may detect if the visitor has accepted the marketing category in the cookie banner. This cookie is necessary for GDPR-compliance of the website.
 - (b) Statistics cookies: help website owners to understand how visitors interact with websites by collecting and reporting information anonymously. These cookies may register data on visitors' website-behaviour, collect statistics on the user's interaction with the real-time price- and stock bar on the website.
 - (c) Marketing: are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and thereby more valuable for publishers and third-party advertisers.
6. In some special cases service providers also use cookies provided by trusted third parties. Third-party analytics are used to track and measure usage of website so that service providers can continue to produce engaging content. These cookies may track things such as how long users spend on the site or pages they visit, which helps them to understand how they can improve the site for you as users.
7. Regularly, service providers may test new features and make subtle changes to the way the site is delivered, during this period, these cookies may be used to ensure that users receive a consistent experience on the site.

Article §11: Storage of Personal Data

1. We store your Personal Data securely using appropriate technical and organizational measures to protect it from unauthorized access, loss, or misuse. The storage and processing of your Personal Data comply with applicable laws, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).



2. Your Personal Data may be stored on servers located within the European Economic Area (EEA), the United States, or other jurisdictions where we or our trusted service providers operate. We take measures to ensure that the location of storage complies with applicable data protection regulation.
3. We implement a range of security measures to safeguard your data, including:
 - (a) Encryption: Personal Data is encrypted both in transit and at rest where applicable.
 - (b) Access Controls: Access to your Personal Data is restricted to authorized personnel only.
 - (c) Regular Security Audits: Our systems and processes are regularly reviewed to identify and address vulnerabilities in line with our certification.
4. We retain your Personal Data only for as long as necessary to fulfill the purposes for which it was collected, as outlined in Clause “Data Retention”. When the retention period expires, or the data is no longer required, it will be securely deleted or anonymized.
5. We may use trusted third-party service providers for data storage. These providers are contractually obligated to ensure the confidentiality and security of your data in accordance with applicable laws
6. Your Personal Data may be stored in encrypted backups to ensure business continuity and disaster recovery. Backup data is securely stored and accessible only to authorized personnel.
7. In certain circumstances, we may be required to retain your Personal Data longer to comply with legal obligations, such as financial reporting or regulatory requirement.



SCHEDULE 1: California Notice at Collection

This California Notice at Collection is provided to residents of California under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA). It outlines the categories of personal information we collect, the purposes for which the information is collected, and whether the information is sold or shared.

CONTENTS:

1. GENERAL PROVISIONS AND CATEGORIES OF PERSONAL DATA COLLECTED
2. PURPOSE FOR WHICH PERSONAL DATA IS COLLECTED AND USE
3. HOW LONG WE RETAIN YOUR PERSONAL INFORMATION
4. YOUR RIGHTS AND CHOICES
5. HOW TO OPT-OUT OF SALE OR SHARING
6. CHANGES TO THIS NOTICE
7. HOW TO CONTACT US

1. GENERAL PROVISIONS AND CATEGORIES OF PERSONAL DATA COLLECTED

- 1.1. This California Notice at Collection is an integral part of our Privacy Notice and applies exclusively to residents of California. This notice does not apply to residents of other states or countries.
- 1.2. In the event of any discrepancies between this notice and the general Privacy Notice, the terms of this California Notice at Collection for residents of California shall prevail.
- 1.3. In accordance with Section 1798.130 of the CCPA, we are obliged to use certain category names to describe the data types we process and include these descriptions in our Privacy Policy. The table below shows the categories of personal data we collect using the CCPA’s required category names as well as the corresponding data types described in our Privacy Policy:

CATEGORY OF DATA (CCPA-defined)	EXAMPLES FROM OUR PRIVACY POLICY	PURPOSE OF COLLECTION
------------------------------------	-------------------------------------	--------------------------



Identifiers	Full name, date of birth, email address, phone number, government-issued ID (e.g., passport, driver's license).	1) To create and manage your account, provide services, communicate with you, and prevent fraud 2) To verify identity, ensure compliance with KYC requirements, and prevent fraud and illegal activities.
Personal Information (Cal. Civ. Code § 1798.80(e))	Address, contact information, and payment details provided during KYC verification.	To fulfill legal and regulatory obligations, including anti-money laundering (AML) compliance.
Characteristics of protected classifications under California or federal law (i.e., your age and gender)	Age, gender, or other classification data	To comply with legal obligations or customize user experiences
Biometric Information	Profile pictures, photographs from IDs, and facial recognition (if required for verification).	To enhance identity verification processes and prevent impersonation or identity fraud
Internet or Network Activity	Browser type, browsing history, device information, interactions with our website	For analytics, improving services, and ensuring security
Geolocation Data	Approximate location	To provide location-based services or customize content
Inferences	Consumer preferences, interests, or characteristics	To personalize your experience and offer tailored recommendations
Email Open/Click Information	Email and IP address, timestamp of email interaction	To analyze the effectiveness of email campaigns and improve communication
Other information you share	Content you provide in surveys, feedback, or support requests	To improve our services, respond to inquiries, and enhance user satisfaction

2. PURPOSE FOR WHICH PERSONAL DATA IS COLLECTED AND USE

2.1. We collect and use your personal data for the following purposes:

Find Us at <https://sens.love/>

© 2025 Sens (18+). All Rights Reserved

- (a) To provide and maintain our services: Ensuring access to and functionality of the Service.
- (b) To diagnose and resolve issues: Troubleshooting and fixing technical problems with the Service.
- (c) To develop and improve services: Evaluating and creating new features, technologies, and enhancements.
- (d) For marketing and advertising: Delivering tailored promotional content and campaigns.
- (e) To comply with legal obligations: Meeting legal requirements or responding to requests from law enforcement, courts, or other competent authorities.
- (f) To fulfill third-party contractual obligations: Ensuring compliance with agreements involving third parties.
- (g) To manage intellectual property and content issues: Addressing reports of intellectual property infringement and inappropriate content.
- (h) To handle legal matters: Establishing, exercising, or defending against legal claims.
- (i) For business operations: Conducting planning, reporting, and forecasting activities.
- (j) To ensure security: Keeping the Service safe by detecting and preventing fraud or unauthorized activities.
- (k) To conduct research and surveys: Improving services by gathering insights from research and user feedback.

2.2. For a detailed breakdown of the purpose for which each data type is used, please refer to our Privacy Policy.

3. HOW LONG WE RETAIN YOUR PERSONAL INFORMATION

3.1. The retention period for each category of personal information depends on the purpose of its collection, the requirements of applicable laws, and our legitimate business needs. For example:

- (a) Account Data: Retained for as long as your account remains active or as necessary to provide our services. After account deletion, we retain limited data for a reasonable period to comply with legal obligations or resolve disputes.



- (b) Payment Data: Retained as required by financial regulations, such as tax or anti-money laundering laws, typically between 5 and 10 years.
- (c) Usage Data: Retained for shorter periods for service improvement and security, unless anonymized for statistical purposes.
For more details, see Section "Data Retention" of our Privacy Policy.

4. YOUR RIGHTS AND CHOICES

- 4.1. As a California resident, you have specific rights regarding your personal information under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):
- (a) The Right to Know: You can request details about the personal information we collect, use, and disclose, including the categories of data and purposes of processing.
 - (b) The Right to Request Deletion: You may ask us to delete your personal information, subject to legal exceptions (e.g., compliance with regulatory obligations).
 - (c) The Right to Opt-Out of Sale or Sharing: You have the right to opt-out if your data is shared for cross-context behavioral advertising.
 - (d) The Right to Correct: You can request correction of inaccurate personal information we hold about you.
 - (e) The Right to Limit Use and Disclosure of Sensitive Information: You may restrict the use of sensitive personal information (e.g., financial data) for specific purposes.
- 4.2. To exercise these rights, you may contact us at **official@sens.love**. We will respond to your request in accordance with applicable laws and within the specified timeframes. For more details on your rights, refer to our Privacy Policy.

5. HOW TO OPT-OUT OF SALE OR SHARING

- 5.1. While we do not sell personal information as defined by the CCPA, we may share your personal information with third parties for purposes such as cross-context behavioral advertising. **You can exercise your right to opt out of that sharing at any time by following the Opt Out Choices links above. Please contact us at** official@sens.love.
- 5.2. If you choose to opt out, we will honor your preference in all applicable circumstances. Note that you may need to renew your opt-out settings if you clear your cookies or use a different device or browser.
- 5.3. Please note that if you choose to opt out of the sale or sharing of your personal information, certain features of our services may no longer function as intended or may be less personalized.



6. CHANGES TO THIS NOTICE

- 6.1. We may occasionally make changes to this Notice.
- 6.2. When we make material changes to this Notice, we'll provide you with prominent notice as appropriate under the circumstances. For example, we may display a prominent notice within the Website or send you an email or device notification.

7. HOW TO CONTACT US

- 7.1. For any questions or concerns about this Notice, contact our Data Protection Officer any one of these ways:
Email: official@sens.love

SCHEDULE 2: GDPR COMPLIANCE NOTICE

This GDPR Compliance Notice is provided to **residents of the European Economic Area (EEA) in accordance with the General Data Protection Regulation (GDPR)**. It outlines the categories of personal data we collect, the purposes for which the data is processed, and the safeguards in place for international transfers of personal data.

CONTENTS

1. GENERAL PROVISIONS
2. INTERNATIONAL TRANSFERS OF PERSONAL DATA
3. POTENTIAL RISKS OF TRANSFERS OUTSIDE THE EEA
4. SAFEGUARDS FOR INTERNATIONAL TRANSFERS
5. EXPLICIT CONSENT FOR TRANSFERS
6. STORAGE AND TRANSFER PRACTICES OUTSIDE THE EEA
7. CONTACT US

1. **GENERAL PROVISIONS**

- 1.1. This GDPR Compliance Notice is provided to residents of the European Economic Area (EEA) in accordance with the General Data Protection Regulation (GDPR).
- 1.2. This GDPR Compliance Notice is an integral part of our Privacy Notice and applies exclusively to residents of the EEA. **It does not apply to residents of other countries or regions outside the EEA.**
- 1.3. In the event of any discrepancies between this notice and the general Privacy Notice, the terms of this GDPR Compliance Notice for residents of EEA shall prevail.
- 1.4. We may occasionally make changes to this Notice. When we make material changes to this Notice, we'll provide you with prominent notice as appropriate under the circumstances. For example, we may display a prominent notice within the Website or send you an email or device notification.

INTERNATIONAL TRANSFERS OF PERSONAL DATA

- 1.5. In accordance with Article 49(1)(a) of the GDPR, your Personal Data may be transferred to our partners located outside the European Economic Area (EEA). These countries may not

provide the same level of data protection as the laws of your country of residence. To ensure compliance with GDPR, we take the following measures:

- (a) **Standard Contractual Clauses (SCCs):** We enter into contractual agreements with partners based on EU-approved clauses, which provide a legal basis for the transfer and adequate safeguards.
- (b) **Partner Compliance:** We only share your Personal Data with third-party partners if they demonstrate compliance with GDPR standards.

2. POTENTIAL RISKS OF TRANSFERS OUTSIDE THE EEA

2.1. Although we and third-party partners take all reasonable and necessary measures to protect your Personal data from unauthorized access by third parties, we must inform you about the potential risks of such storage of your Personal data within jurisdictions outside of the EEA in accordance with Article 49 (1) (a) GDPR. By agreeing to processing of your Personal data in accordance with this Privacy Policy, you give us explicit consent to transfer of your Personal data to jurisdictions outside the EEA, despite all possible risks of such transfer. Among such potential risks are:

- (a) **Different Regulatory Standards.** Existence of rules and regulations on processing of Personal data in such jurisdictions other than GDPR. Despite this, we provide Personal data subjects with the level of guarantees provided to Personal data subjects by GDPR.
- (b) **Access by Government Authorities.** Local government agencies may access your Personal Data, but only in compliance with applicable local laws and on legitimate grounds. We minimize disclosures to the extent legally permissible and challenge disproportionate requests where possible.
- (c) **Obtaining access to your Personal data by government agencies.** However, such access can be obtained by these authorities only in accordance with the current legislation of the relevant country and if there are legal grounds for obtaining access. We undertake not to disclose data in absence of a legitimate reason and to do so only to the minimum extent necessary for this. Attempts to illegally access Personal data. We take all the necessary measures to prevent such attempts and prevent unauthorized access to your Personal data.

3. SAFEGUARDS FOR INTERNATIONAL TRANSFERS

- 3.1. To protect your Personal Data during international transfers, we employ the following measures:
- (a) Standard Contractual Clauses (SCCs): Ensuring data transfers to non-EEA countries adhere to EU-approved contractual standards.
 - (b) Risk Assessments: Conducting evaluations of the data protection risks associated with transfers.
 - (c) Enhanced Technical Measures: We may implement advanced encryption, pseudonymization, and secure access controls to protect your data.
 - (d) Additional Policies: Establishing procedures to prevent unauthorized access and ensure that partners meet GDPR compliance standards.

4. EXPLICIT CONSENT FOR TRANSFERS

- 4.1. By agreeing to this Privacy Policy, you explicitly consent to the transfer of your Personal Data to jurisdictions outside the EEA, **including those that may not offer the same level of protection as GDPR**. We ensure:
- (a) Your rights as a data subject are upheld.
 - (b) All transfers occur with the necessary safeguards in place.

5. STORAGE AND TRANSFER PRACTICES OUTSIDE THE EEA

- 5.1. If your Personal Data is stored or transferred outside the EEA, we ensure compliance with GDPR through:
- (a) Standard Contractual Clauses: Providing a legal framework for secure and compliant transfers.
 - (b) Technical and Organizational Measures: Protecting your data through encryption, access restrictions, and periodic audits.
 - (c) Legal Safeguards: Ensuring that third-party partners adhere to contractual obligations for data protection.



PRIVACY POLICY

Last Modified: **DECEMBER 27, 2024**

6. CONTACT US

- 6.1. If you have concerns about how your Personal Data is transferred or wish to learn more about our GDPR compliance measures, please contact us at official@sens.love