Privacy Policy

This privacy policy has been compiled to better serve those who are concerned with how their 'Personally Identifiable Information' (PII) or personal data is being used online.

PII, as described in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Please read our privacy policy carefully to get a clear understanding of how we collect, use, protect or otherwise handle your Personally Identifiable Information in accordance with our website.
‘Personal data’, as defined in General Data Protection Regulation (GDPR) means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What personal information do we collect from the people that visit our blog, website, product or app?

When registering on our site or on our product, as appropriate, you may be asked to enter your name, email address, phone number or other details to help you with your experience. We store these details, but we don't store credit card numbers. We may store credit card details only with your permission and in one of the secured servers of our payment gateway service providers.

On our product website we also use first-party Local Storage Objects to store user and content information to provide certain personalized features.

When do we collect information?

We collect information from you when you register or enter information on our site/product. We also

How do we use your information?

We may use the information we collect from you when you register on our product, make a purchase, sign up for our newsletter, respond to a survey or marketing communication, surf the website, or use certain other site features in the following ways:

- To allow us to better service you in responding to your customer service requests.
- To send periodic emails regarding your order or other products and services.
- To follow up with them after correspondence (live chat, email or phone inquiries)

How do we protect your information?

Your personal information is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems, and are required to keep the information confidential. In addition, all sensitive/credit information you supply is encrypted via Secure Socket Layer (SSL) technology.

We implement a variety of security measures when a user enters, submits, or accesses their information to maintain the safety of your personal information.

For your convenience we may store your credit card information longer than 30 days in order to expedite future orders, and to automate the billing process.

Do we use 'cookies'?

We work with our customers as a data processor in which case we do not use cookies or even require our customers to use cookies with our service. In our corporate website and product sites we use first-party and third-party cookies for analytics purposes, to identify visitors, track website navigation, track email campaign effectiveness, provide support services etc.

Third-party disclosure

We do not sell, trade, or otherwise transfer to outside parties your Personally Identifiable Information.

Third-party links

We do not include or offer third-party products or services on our website.

We have implemented the following:

We, along with third-party vendors such as Google use first-party cookies (such as the Google Analytics cookies) to compile data regarding user interactions on our product site or our partner websites..

Opting out:
Users can opt out by using the Google Analytics Opt Out Browser add on.

Users can visit our site anonymously.

Once this privacy policy is created, we will add a link to it on our home page or as a minimum, on the first significant page after entering our website.
Our Privacy Policy link includes the word 'Privacy' and can easily be found on the page specified above.

You will be notified of any Privacy Policy changes:

- On our Privacy Policy Page

Can change your personal information:

- By logging in to your account

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) is a data protection law instituted by the European Union (EU). This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

GDPR requires that the controller of personal data - either RecoSense, a RecoSense partner or any party, who interfaces with natural persons in the European Economic Area (EEA), inform their end users about their rights, usage of their personal data for processing including - to understand individual user interests by tracking content being consumed by the end user.

The controller, who comes under the purview of GDPR, needs to inform their end users about the following and get explicit consent from them to collect their usage or consumption data for personalization and aggregated user behavior analysis. The user consent should be explicitly passed to RecoSense platform before any user action/events are processed.

Data Security

All the data passed on to RecoSense platform is kept under multiple layers of security few of which are listed below:

- The servers where the data is stored can only be accessed with a secure private key
- The database where the data are kept require authentication for access
- All data files are encrypted and can only be read if decrypted with a key
- When an user data is sent over the internet it is secured and encrypted with an SSL certificate

Right to information / Information Transparency

Your data may be stored and processed in our servers located either of US, Europe or Asia; and also get end user's consent before their data is collected and sent to RecoSense platform.

The personal data and user profiles of users who are not active for more than 3 months would be deleted; and the personal data in the logs and backups would get deleted from the system another 3 months after deletion of the user profiles.

Our customers/partners should communicate to their end users in the EEA about the above and get the end user's content before their data is collected and sent to RecoSense platform.

Right to Access

You may request to view your personal data at any time, or edit the same by signing in to your account. You have an option to request for your personal data and know how it is being processed, at which location, and for what purpose.

If you are a RecoSense customer/partner you should inform your end users that they may request to view their personal data at any time. You need to give the end users an option to access their personal data being processed, how their personal data is being processed, at which location, and for what purpose.

The user specific data can be retrieved from RecoSense platform via an API using a user specific ID.

Right to be Forgotten

End users have complete authority to delete or erase their personal data - profile and event data, permanently from our systems. You can request for the same from within your account, which will also result in the deletion of your account.

Our customers/partners should inform their end users that they have complete authority to delete or erase their personal data - profile and event data, permanently from your systems. You have to give the end users an option to delete their personal data, and inform RecoSense platform of the same via our API using a user specific ID.

Right to Suppress

End users have the right to ask the controller to stop further processing of their personal data. If you have a RecoSense account (on our product or platform) you can make a request to delete your account to stop further processing of your personal data.

If you are a RecoSense customer/partner then you can take the request from your end user to suppress their personal data. it can be informed to RecoSense platform via an API using a user specific ID. When an end user requests to stop processing their data it would same as deleting their personal data from RecoSense platform.

As a controller, it is our customer's responsiblity to stop sending any further data regarding an end user who has requested to suppress or delete their personal data.

RecoSense has updated its products and platforms suitably to meet all of the above requirements, and now provides APIs (Application Programming Interfaces) to its customers, who are collectors of data, to in turn meet their obligations under GDPR towards their end users.

You can refer our updated API documentation to understand how to use these APIs.

How does our site handle Do Not Track signals?
We do not currently honor 'Do Not Track' signals sent out from certain internet browsers as there is no standard for the same. When a universal standard for processing 'Do Not Track' signals emerges, we will follow it.

Does our site allow third-party behavioral tracking?
We do not allow third-party behavioral tracking.

Children's Personal Information
We do not specifically market to children under the age of 13 years old. Our products and services are not meant for children. RecoSense does not knowingly collect personal information from children. If we become aware that a child under 13 has provided us with personal information, we will take steps to delete such information. If you believe that a child under 13 years has provided personal information to us, please write to us at support@recosenselabs.com with the necessary details, and we will take the required steps to delete the information we hold about that child.

Fair Information Practices

The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information.

In order to be in line with Fair Information Practices we will take the following responsive action, should a data breach occur:

- Within 7 business days

We will notify the users via in-site notification

- Within 7 business days

Data Processing Agreement or Contract

To enable you to be compliant with the data protection obligations under the GDPR, we can sign a data processing contract that is based on standard contractual clauses. You can contact us at support@recosenselabs.com or your account manager for a copy of the contract.

We also agree to the Individual Redress Principle which requires that individuals have the right to legally pursue enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or government agencies to investigate and/or prosecute non-compliance by data processors.

For more information about our privacy, data processing and security policies please email us at support@recosenselabs.com or contact your account manager.