



Draup

Data Privacy Policy

Purpose

This policy presents the Draup (herein referred to as organization) commitment to the privacy of user information and sensitive commercial/financial data.

Scope

This policy applies to all data owned or managed by Draup (herein referred to as organization).

Definition

- ISMS: Information Security Management System
- IP Address : A unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.

Responsibilities

1. The chief information security officer (CISO) is responsible for developing, implementing, maintaining, and enforcing the policy.
2. Employees are responsible and/or accountable to ensure adherence to this policy's terms during their job duties.

Policy

The privacy policy displayed to the user must clearly communicate a minimum of the following information:

- The purpose for the collection of personal information.
- How will the information be processed?
- Controls for the protection of personal information.
- Usage of tools such as cookies to collect personal information online.
- Details of information, such as IP address, and domain information, are captured about the user.
- Sharing of information with third parties.
- User rights to access personal information.
- Details to contact the organization for queries on processing personal information.
- Organization's commitment to privacy and security.

- Period for which the terms and conditions are valid.
- Organization's information security standards and practices.

Policy on external links

- Organizations will not use information about user activities on the internet together with any information that would result in the user being identified without their consent.
- Organizations will not associate the information collected by software utilities (cookies, single-pixel gif images) with the username or email address when the user visits the sites.
- The organization will implement policy guidelines to safeguard the privacy of the user-identifiable information from unauthorized access or improper use. It will continue to enhance security procedures as new technology becomes available.
- Organizations honor requests from users to review all personally identifiable information, such as names, addresses, e-mail addresses, and telephone numbers, maintained in reasonably retrievable form. It will correct inaccurate information that the users may verify.
- Organizations may use the user's identifiable information to investigate and help prevent potentially unlawful activity or activity that threatens the network or otherwise violates the user agreement for that service.
- All kinds of data, such as personally identifiable information shared by users, shall be:
 - Processed fairly, lawfully, and securely.
 - Processed per the purpose for which it is collected.
 - Maintained up-to-date and accurate as necessary.
 - Retained for no longer than necessary for the purpose it is collected.
- Users shall be provided with the following information, at the least, before collecting personally identifiable information
 - Purposes of processing the information.
 - Information regarding the specific circumstances in which personal information is collected, such as
 - The recipients of the information.
 - Whether submission of information is obligatory or voluntary, as well as the impact of failure to submit such information.
 - The right to access, update, or remove personal information exists.
 - Whether personal information will be used for marketing purposes.

Data Privacy Policy

Version	v1
Created By	Scrut Team, Mar 17, 2025
Approved By	Kashish, Apr 1, 2025
Published By	Kashish, Apr 1, 2025