mouseflow

PRIVACY WHITEPAPER

10 Key Things to Know About Mouseflow's Data Practices

1. Purpose of this Privacy Whitepaper

This Whitepaper provides an overview of Mouseflow's data processing practices, ensuring legal teams understand our privacy framework before reviewing our Data Processing Agreement (DPA) and Master Services Agreement (MSA). Our goal is to offer transparency and avoid misunderstandings regarding how data is collected, stored, and processed.

2. Summary of key privacy commitments

Mouseflow is designed with privacy in mind and adheres to global data protection laws. Our key commitments include:

3. Purpose of data collection

Mouseflow collects data to help its Customers understand user behavior on their websites. This enables website owners to improve usability, identify bottlenecks, and optimize overall performance. Our platform captures anonymized or pseudonymized information wherever possible to minimize privacy risks. The data collected is used solely for the purposes outlined in our agreements with the Customer and is not sold or shared to any third parties.



No personal data collection by default

Mouseflow operates with privacy-by-design principles, ensuring minimal data collection.



No third-party tracking or cross-site tracking

We do not use third-party cookies or track visitors beyond the Customer's website.



Customer-controlled data collection

Customers must use our Visual Privacy Tool and code settings to ensure personal data is not recorded.



Robust security and encryption

TLS encryption in transit, AES encryption at rest, and ISO 27001 and SOC 2 Type II certified data centers.



Compliance with Global Privacy Laws

GDPR, CCPA, LGPD, and other applicable regulations.



Customer data ownership

Customers own the data collected on their websites, and Mouseflow acts solely as a data processor - DPA provided.

4. Types of data collected and data minimization

Our services are designed to deliver valuable insights without requiring the collection of personal data, ensuring privacy compliance and adherence to data minimization principles. We collect technical and behavioral data, such as browser information, device type, and user interactions, to provide actionable insights while respecting website visitors' privacy.

Please visit this Help Article, for more information about the data collected by Mouseflow.

What we do NOT collect by default:

- No passwords or financial information.
- No keystroke logging in form elements.
- No full IP address storage.
- No third-party tracking.
- No recording of elements excluded by the Customer in the the Privacy Tools provided by Mouseflow.

What we collect:

- Behavioral Data: Clicks, scrolls, interactions, heatmaps.
- Technical Metadata: Browser type, device type, operating system.
- Geolocation Data: High-level geolocation (state/country level only). Full IP addresses are not stored.



Customer responsibilities & privacy configuration:

Customers are responsible for ensuring compliance with our terms and the data protection laws when using Mouseflow. To uphold privacy standards:

Mandatory use of Privacy Tools:

Customers must configure our Visual Privacy Tool to exclude any elements containing user identifiers or other personal data.

Consent management:

Customers must ensure they provide website visitors with a clear privacy notice, informing them of Mouseflow's use (see our template here), and must obtain the necessary consents, as required by the privacy laws. Mouseflow can integrate with third-party consent management platforms.

Testing before recording:

Customers are required to verify before enabling recording that all personal data is properly excluded, ensuring compliance with our terms and privacy regulations.

For more details about protecting website visitors' privacy, visit this Help Article.

5. Data Security & Compliance

Mouseflow prioritizes security through multiple layers of protection:

- Encryption: TLS encryption in transit and AES encryption at rest.
- Certifications: ISO 27001 and SOC 2 Type II certified data centers.
- Security audits: Annual penetration tests performed by third party and quarterly vulnerability scans.
- Access controls: SSO, MFA, and strict password policy can be applied.

6. First-Party Cookies

Mouseflow exclusively uses first-party statistic cookies with an expiration period of no more than 90 days. These cookies are used solely for analytics and performance insights. We do not use third-party cookies, nor do we track visitors across websites. See the current list of cookies used by Mouseflow in this Help Article.

When enabled by the Customer, our cookieless solution utilizes SessionStorage and LocalStorage technologies instead of cookies.
For more information, see this Help Article.

7. Data ownership and Data Processing Agreement

Data collected through Mouseflow belongs to our Customers. Mouseflow processes data solely on behalf of Customers and in line with their instructions, as outlined in the Data Processing Agreement (DPA).

8. Data retention

Mouseflow retains data for the duration specified in the Customer's subscription plan, up to a maximum of 13 months. Customers can request data deletion at any time.

9. Compliance with Privacy Laws globally

Mouseflow is designed with global privacy laws in mind, including GDPR, US Privacy Laws (e.g., CCPA, VCDPA), and LGPD, with a strong emphasis on data minimization and privacy by design. Our platform is built to avoid the collection of personal data. To support compliance, we offer features such as integration with cookie consent management tools and customizable tracking options that enable Customers to exclude personal data and focus solely on technical and behavioral insights.

10. Subprocessors & Cross-Border Transfers

To provide services, Mouseflow relies on essential subprocessors, all of whom undergo strict vetting to meet our security and compliance standards.
Unless otherwise directed by the Customer, data storage follows these rules:

- EU Customers: Data is stored in the EU.
- US Customers: Data is stored in the US.
- International Transfers: where necessary, Mouseflow ensures compliance with SCCs (Standard Contractual Clauses) and the EU-US DPF (Data Privacy Framework) for data transfers outside the EU.

A full list of our subprocessors is available here.

Contact & Further Information

Mouseflow has a dedicated privacy team that monitors regulatory changes and ensures compliance. If you require additional information or have specific legal questions, please contact us at privacy@mouseflow.com.



Disclaimer

The information provided in this Whitepaper is for general informational purposes only and does not constitute legal advice. Nothing in this document supersedes our official privacy policies, Data Processing Agreement, Terms of Use or Mouseflow Subscription Agreement.