Privacy By Design

Data Masking and High Value Encryption

In today's digital world, personal data is a valuable commodity that allows your business to offer targeted products and services that meet your customers' needs. While reflecting this tremendous value, the digital collection of personal data has never been under closer scrutiny.

We understand the challenges that organizations are facing in today's world following the institution of privacy regulations like GDPR and the increasing need to respect data privacy. With this in mind, Glassbox was founded on the principle that the security and privacy of customer data are paramount.

In order to provide you with peace of mind and enable you to comply with all relevant regulatory requirements Glassbox integrates multiple security layers and specific rules to protect personal data.

GLASSBOX

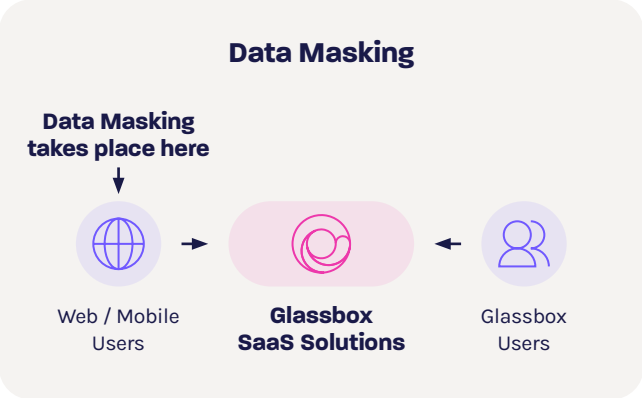
Glassbox Privacy Controls

Our advanced digital data privacy capabilities empower customers to either mask their data or apply high-value encryption at any level—from end-user to system-wide—including all relevant cardholder and personal information. These capabilities guarantee that no sensitive data is captured and processed by Glassbox, ensuring our customers' compliance with all applicable privacy regulations.

Glassbox has implemented comprehensive policies and procedures to protect its customer's personal data in compliance with all applicable privacy regulations. Glassbox is the only company in our domain that holds the ISO/IEC 27701 certification, which demonstrates our high level of commitment to data protection and compliance with key international regulations, including GDPR, CRPA and more.

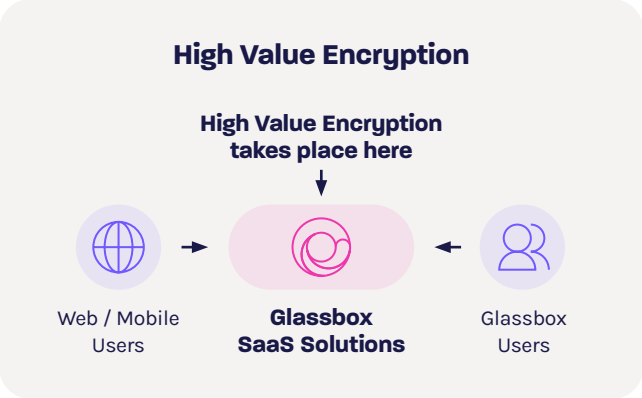
Data Masking

With data masking, personal data can be removed from the captured session **before** it ever leaves the user's device. You can decide in advance which data is sent to the cloud and prevent any personal data from being captured.



High Value Encryption

Encrypting personal data involves converting it into a secure format that is only accesible to authorized individuals. This process is required by several industries due to the sensitivity of the data. The process ensures that the data is only visible according to pre-set rules or roles and we allow customers to control and restrict data replay within their organization to specific roles, according to their business needs.



Whitelist

To support our high value encryption and masking capabilities and reduce human error to ensure full compliance, Glassbox employs a whitelist approach for capturing all input fields on customers' digital services. This means that right from the start, all information captured from input fields is automatically masked, aligning with your preferences.

PCI & Personal Data Automatic Omission

Finally, as an extra precaution to guarantee no unwanted information is ever saved,, we utilize our automatic PCI and personal data removal tool.Configured according to your requirements, it will automatically detect, alert and process unwanted information, fully guaranteeing your compliance with privacy regulations.

Data Privacy is fully supported in both our mobile SDK and JavaScript

- Whitelist/blacklist
- Screen-level masking
- Component-level masking
- All INPUT fields

- Whitelist/blacklist
- Based on specific class\ID
- DOM Masking – Masking the entire screen by default, showing only predefined elements (Glassbox exclusive capability)

Nature of Relationships

Glassbox operates as a data processor for its customers and does not have any direct relationship with individual data subjects, working solely according to our customers' instructions. The sole controller of the gathered data is the applicable Glassbox's customer. Glassbox operates in accordance with the customer, empowering them to meet any privacy regulations requirements.

In line with client preferences, Glassbox only collects PII that has not been masked by our privacy controls. We recommend minimizing the collection of personal data, adhering to the GDPR data minimization principle.

Glassbox will communicate any requests received from data subjects relating to the captured personal data and shall not respond to such communications unless we have been expressly authorized to do so by the customer, in accordance with applicable privacy laws.

GLASSBOX

Purposes of the Processing

Glassbox assists its customers with multiple use cases such as understanding and optimizing the user journey, detecting fraud, finding IT and security flaws in their digital service and keeping records for compliance with their applicable regulations. The processing of data is mostly intended to improve the overall digital services our customers provide to their end users.

Scope of the Processing

The nature of the data may vary in accordance with the customer's services and business preference. The platforms can track the user's journey in customers' digital services and in the process may capture information that was inputted by the user during their journey. This data may be of sensitive nature, such as PCI information, sensitive personal data (in accordance with the definition of the GDPR) and additional personal and non-personal data.

Glassbox out-of-the-box Privacy Controls.

Data Minimization

In order to prevent any excessive data gathering, Glassbox has developed tools to ensure that the collection of personal data is kept to a minimum. Among these tools are:

- **Masking:** This prevents data from leaving the end user's device.
- **IP Removal:** Allows for the identification of a geographical area but not the individual subject's location.
- **High Value Encryption:** When personal data is captured, the high value encryption tool allows minimized access to data in accordance with pre-determined role.
- **Personal Data and PCI Auto Remover:** Identifies and removes specific patterns of sensitive data automatically.
- **Data Location:** Choose from Glassbox's multiple global cloud locations and set your data location in advance,ensuring no data is transferred.
- **Whitelist Input Fields:** Gather only the data you have actively chosen to collect.

Data Transfers

The collected data is not shared with third parties unless specifically requested by the customer. Glassbox offers the ability to integrate with multiple 3rd party tools, but these tools are not provided access to customer personal data. All data resides behind an authentication wall.

Data Storage Locations

The data can be stored on AWS or Azure servers in multiple global locations, in accordance with the customer's preferences and requirements. Among Glassbox's current locations are:

- US East (N. Virginia) (AWS/Azure)
- Ireland (AWS/Azure)
- Hong Kong (AWS)
- Canada (AWS/Azure)
- Australia (AWS)
- Singapore (AWS/Azure)

Data Retention

The data is kept in accordance with the applicable customer's requirements and is aligned with Glassbox's data retention policy, as described below:

Session Replay	Data for Session Replays and data for Interaction Maps.	Options: 1 month up to 12 months
Analytics	Data for Page Analysis, Business Flows, Error Reports, Mobilebox, Augmented Journey Map™, User Timeline and CX Perform.	Options: 1 month / 3 months / 6 months / 13 months
VoS	Data for Voice of the SilentFeedback.	13 months (fixed)
Ad-Hoc Reports	Data for reports, Funnels, Alerts, Anomalies and Pre-calculation Reports.	Options: 1 month / 3 months / 6 months / 13 months
Session Vault	When using our vault module, a specific session can be saved in accordance with present attributes, allowing you to keep the necessary data in accordance with the required business purpose.	As long as needed

Technical Security Measures

Glassbox has implemented robust technical and organizational safeguards in accordance with industry best practices. To learn more about the technical and organizational security measures implemented by Glassbox please visit our security and privacy homepage.