

GDPR Compliance Statement for Scared So What Ltd and C.I.C.

Introduction

Scared So What is committed to protecting the privacy and security of our users' personal data. This GDPR Compliance Statement outlines our practices and commitments in accordance with the General Data Protection Regulation (GDPR). Our data processing activities are designed to respect user privacy and ensure the lawful, fair, and transparent handling of personal data.

Data Processing Activities for "Scared So What"

Data Collection

"Scared So What" collects personal data from employees to support their journey through personal change. This data includes, but is not limited to:

- **User-Generated Content:** Information entered by users about their personal change experiences, goals, and reflections.
- **Engagement Data:** Information on how users interact with the app, including features used and content accessed.
- **Consent Records:** Documentation of when and how users have given their consent for data processing.

Data Use

The personal data collected is used exclusively for the following purposes:

- **Personal Development:** To facilitate and track users' personal change journeys, offering customized content and recommendations.
- **App Improvement:** To analyze how users interact with the app, identifying areas for enhancement to improve user experience.
- **User Support:** To provide assistance and respond to user inquiries or feedback.

Data Hosting and Security

All personal data is hosted within the EU/UK, ensuring compliance with GDPR's stringent data protection requirements. "Scared So What" employs robust security measures to safeguard personal data, including:

- **Encryption:** All data is encrypted during transmission and at rest.
- **Access Control:** Strict access controls are implemented to ensure that only authorized personnel can access personal data, and only for legitimate purposes.
- **Regular Audits:** Regular security audits are conducted to identify and remediate potential vulnerabilities.

Data Sharing and Disclosure

“Scared So What” does not share personal data with third parties without explicit user consent, except in circumstances required by law. Within a company, data may be shared with management or senior stakeholders only if the user chooses to share their personal change data. Such sharing is governed by clear consent mechanisms within the app.

Consent Management

Users are provided with clear, accessible information on how their data will be used and are required to give explicit consent before any data processing begins. Users have the ability to withdraw their consent at any time through the app’s settings.

Data Retention and Deletion

Personal data is retained for as long as necessary to fulfill the purposes outlined in this document, or until the user requests deletion of their data. Upon a user leaving a company or if a user decides to delete their account, their personal data is retained in a secure manner for a predefined period to comply with legal obligations and then securely deleted.

Purpose of Data Collection

Purpose of Data Collection for “Scared So What”

The collection of personal data in “Scared So What” is driven by a commitment to support employees through their personal change and development journey, with the utmost respect for their privacy and autonomy. The specific purposes for collecting personal data are as follows:

Supporting Personal Change

- **Customized Experience:** To tailor the app’s functionalities and content according to the individual’s personal change goals, progress, and preferences, thereby enhancing their journey towards personal growth and development.
- **Goal Setting and Tracking:** To facilitate the setting of personal objectives and monitor progress over time, enabling users to reflect on their growth and areas for improvement.

Enhancing User Experience

- **App Optimization:** To understand how users interact with the app, which sections or features are most engaged with, and where improvements can be made to make “Scared So What” more user-friendly and effective.
- **Feedback Implementation:** To collect and act on user feedback, ensuring that the app evolves in ways that meet the users’ needs and expectations.

Facilitating User Engagement

- **Communication:** To enable effective communication with users about updates, new features, or personalized insights related to their personal change journey.
- **Community Building:** To foster a sense of community among users by optionally allowing them to share their experiences and successes with peers within the app, should they choose to opt into such features.

Legal and Regulatory Compliance

- **Consent Verification:** To ensure that all data collection and processing activities are conducted in full compliance with GDPR, including maintaining records of when and how consent was given by users.
- **Security and Privacy Protections:** To implement and maintain high standards of data security and privacy, in line with GDPR requirements, and to communicate clearly with users about their rights and how they can exercise them.

Research and Development

- **Innovative Features:** To research and develop new features, tools, and resources that can support users' personal change journeys more effectively, based on the analysis of aggregated and anonymized data patterns.

The personal data collected by “Scared So What” serves to empower employees in their personal development, ensuring a respectful, secure, and beneficial use of their information. At every step, users have full control over their data, including the right to access, rectify, and delete their information, further reinforcing our commitment to their privacy and GDPR compliance.

Data Protection Measures

Data Protection Measures for “Scared So What”

“Scared So What” is committed to implementing and maintaining the highest standards of data security and privacy for our users. Recognizing the sensitive nature of personal data related to personal change, we have instituted the following measures to ensure data protection:

Encryption

- **Data Encryption:** All personal data, both at rest and in transit, is encrypted using state-of-the-art encryption technologies. This ensures that user data is secure and unreadable to unauthorized parties.

Access Control

- **Strict Access Policies:** Access to personal data is strictly limited to authorized personnel who require it to perform their job functions. We employ a least privilege policy, ensuring individuals have access only to the data necessary for the task at hand.
- **Authentication and Authorization:** We implement robust authentication mechanisms to verify the identity of users and personnel, coupled with authorization checks to ensure they can access only what they are permitted to.

Data Anonymization

- **Anonymization of Data:** Where possible, data is anonymized or pseudonymized to protect user privacy, especially in the context of analytics and app improvement activities. This ensures that personal information cannot be linked back to any individual without additional information that is kept separately under strict security.

Security Training and Awareness

- **Regular Training:** All employees receive regular training on data protection and privacy principles, ensuring they understand their responsibilities in safeguarding user data.
- **Awareness Programs:** We run ongoing awareness campaigns to keep data protection at the forefront of our employees' minds, fostering a culture of security within the organization.

Incident Response and Data Breach Procedures

- **Incident Response Plan:** We have a comprehensive incident response plan in place to quickly address any suspected data breaches or security incidents, minimizing any potential impact on user data.
- **Notification Procedures:** In the event of a data breach, we are prepared to notify affected users and relevant authorities promptly, in accordance with GDPR requirements.

Regular Audits and Compliance Checks

- **Security Audits:** Regular security audits are conducted to assess the effectiveness of our data protection measures, identify potential vulnerabilities, and implement corrective actions.
- **Compliance Monitoring:** Continuous monitoring and reviews are performed to ensure that our data handling practices remain in full compliance with GDPR and other relevant data protection regulations.

Data Hosting and Processing

- EU/UK Data Hosting: All personal data is hosted in secure data centers located within the EU/UK, ensuring that it benefits from the protections afforded by GDPR.
- Vendor Assessments: Any third-party vendors or service providers are thoroughly assessed to ensure they meet our stringent data protection and privacy standards.

“Scared So What” is deeply committed to protecting the privacy and security of our users’ personal data. Through these comprehensive data protection measures, we strive to not only comply with GDPR but to exceed the standard expectations of data privacy and security, ensuring our users can trust us with their personal change journeys.

User Rights

User Rights under GDPR for “Scared So What”

“Scared So What” respects and upholds the rights granted to users under the GDPR. We are committed to ensuring that users can exercise these rights easily and transparently. As a user of “Scared So What,” you have the following rights regarding your personal data:

Right to Be Informed

You have the right to be informed about the collection and use of your personal data. This includes understanding how your data is collected, used, and shared, all of which is detailed in this GDPR compliance statement and our privacy policy.

Right of Access

You can request access to your personal data to verify the lawfulness of processing. This means you can ask for a copy of the personal data we hold about you.

Right to Rectification

If you find that the personal data we hold about you is inaccurate or incomplete, you have the right to have it corrected or completed without undue delay.

Right to Erasure (Right to Be Forgotten)

You have the right to request the deletion or removal of your personal data where there is no compelling reason for its continued processing. This includes situations where the data is no longer necessary in relation to the purposes for which it was collected or processed.

Right to Restrict Processing

You have the right to ‘block’ or suppress the processing of your personal data under certain conditions, such as when you contest the accuracy of the data or when you have objected to processing.

Right to Data Portability

You have the right to obtain and reuse your personal data for your own purposes across different services. This means you can transfer your data from “Scared So What” to another service in a safe and secure way, without hindrance to usability.

Right to Object

You have the right to object to the processing of your personal data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing, and processing for purposes of scientific/historical research and statistics.

Rights Related to Automated Decision Making and Profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you, unless necessary for entering into, or performance of, a contract between you and “Scared So What” or based on your explicit consent.

How to Exercise Your Rights

To exercise any of these rights, please contact us using the contact details provided in our app or website. We will respond to your request in accordance with GDPR requirements, typically within one month of receiving a valid request.

Data Retention and Deletion

Personal data is retained only for as long as necessary for the purposes for which it was collected. Users have the right to delete their data at any time through Scare So What . Upon termination of employment, an individual’s data will continue to be protected under GDPR, and Scared So What will ensure that the data is handled in accordance with the user’s rights and our data retention policies.

Data Sharing and Transfer

Data Retention and Deletion for “Scared So What”

At “Scared So What,” we are committed to the principles of data minimization and limiting data retention, ensuring that personal data is kept no longer than necessary for the purposes for

which it is processed. Our data retention and deletion policies are designed to respect user privacy and comply with GDPR requirements.

Data Retention

- **Personal Change Data:** Data related to personal change journeys, including goals, reflections, and progress, is retained as long as the user account is active or as needed to provide services to the user.
- **User Account Information:** Basic user account data is kept for the duration of the user's engagement with "Scared So What." Should a user decide to deactivate or delete their account, their personal data is removed in accordance with our deletion procedures.
- **Legal and Regulatory Requirements:** In some cases, we may be required to retain certain information for longer periods to comply with legal, tax, or regulatory requirements.

Deletion Procedures

- **User-Requested Deletion:** Users have the right to request the deletion of their data at any time. Upon receiving a deletion request, "Scared So What" will remove the user's personal data from our active databases and any other records, subject to any legal or regulatory requirements that require data retention.
- **Automatic Deletion:** Inactive user accounts and associated data may be automatically deleted after a certain period of inactivity, following notification to the user.
- **Secure Deletion:** When deleting personal data, "Scared So What" employs secure deletion methods to ensure that data is irrecoverably erased and cannot be reconstructed or retrieved.

Data Delegation

- **Upon Termination of Employment:** If a user's employment is terminated or they leave the company using "Scared So What" under license, their data will remain protected under GDPR. Employers will not have access to an individual's data without their consent, and the user can request deletion of their data.
- **Data Transfer Requests:** Users have the right to data portability, allowing them to request the transfer of their personal data to another service. "Scared So What" facilitates this process in a secure and efficient manner, ensuring data integrity and confidentiality.

Maintaining Data Integrity and Privacy

"Scared So What" is dedicated to maintaining the highest levels of data integrity and privacy. Our data retention and deletion policies are regularly reviewed and updated to comply with current data protection laws and best practices.

Data Sharing and Transfer for "Scared So What"

“Scared So What” prioritizes the privacy and security of our users’ personal data. We adhere strictly to GDPR principles, ensuring that any sharing or transfer of data is conducted with the utmost care and only under specific conditions:

Sharing within Licensed Companies

- **Management and Senior Stakeholders:** Personal change data entered by users is primarily for their own use and development. It may be shared with management or senior stakeholders within the user’s company only if the user explicitly opts to share this information. Such sharing is designed to foster personal growth and professional development opportunities.

Third-Party Service Providers

- **Operational Support:** “Scared So What” partners with selected third-party service providers for essential operational services, such as hosting, data analytics, and customer support. These providers are carefully chosen and bound by confidentiality agreements to ensure they handle data securely and in accordance with GDPR.
- **Compliance with Legal Requests:** In certain circumstances, “Scared So What” may be required to disclose user data in response to lawful requests by public authorities, including meeting national security or law enforcement requirements.

International Data Transfers

- **EU/UK Data Hosting:** All personal data is hosted in the EU/UK, adhering to GDPR data protection standards. Should any transfer of data outside the EU/UK be necessary, “Scared So What” ensures that such transfers are carried out in compliance with GDPR, employing mechanisms like Standard Contractual Clauses or ensuring the receiving country has been deemed adequate by the European Commission.

Consent and Control

- **User Consent:** Except as described above, no personal data is shared with any third parties without the explicit consent of the user. Users retain control over their data and can adjust their sharing preferences at any time through the app’s settings.

Security Measures in Data Transfer

- **Safeguarding Data:** In any instance where data is shared or transferred, “Scared So What” employs rigorous security measures and encryption to protect the data against unauthorized access or breaches.

Changes to Our Sharing Practices

- Notification of Changes: If there are any changes to how “Scared So What” shares personal data, users will be notified through updates to this GDPR compliance statement or directly via email or app notifications, ensuring transparency and giving users the opportunity to review and adjust their preferences.

Changes to Our GDPR Compliance Statement

We may update this statement from time to time to reflect changes in our practices or legal requirements. Users will be notified of any significant changes.

Contact Information

For any questions or concerns regarding this GDPR Compliance Statement or our data protection practices, please contact us at info@scaredsowhat.com