Fyxer.ai

Data Protection Policy

Version 1 - Approved by Richard Hollingsworth

Contents

1. Objective
2. Scope
3. Policy Statement
4. Principles for Processing Personal Data
5. Security of Personal Data
6. Data Subject Rights
7. Staff Training
8. Data Protection Officer
9. Document Security Classification
10. Non-Compliance
11. Responsibilities
12. Schedule
13. Version history

1. Objective

Fyxer AI is committed to protecting the privacy of personal information and to compliance with data protection laws. The purpose of this policy is for all Fyxer AI staff members to understand their responsibilities toward protecting the privacy of personal and sensitive information that we collect and process as part of our operations.

2. Scope

This document is applicable to all processes and operations in Fyxer AI within the scope of the ISMS.

3. Policy Statement

“Personal Data” refers to any data that relates to an identified or identifiable individual or person. In practice, personal data includes all that can be assigned to an individual in any way. For example, personal data includes a telephone number, credit card number or identification number, account data, number plate, appearance, customer number, or address. This policy lays down guidelines to secure the processing of personal data collected by Fyxer AI, directly or indirectly from the customers and users of Fyxer AI’s services.

4. Principles for Processing Personal Data

At Fyxer AI, we incorporate the following principles of data protection in the way we collect and store personal data. We ensure that the data we collect is:

- Processed lawfully, fairly, and in a transparent manner.
- Collected for specific, explicit, legitimate, and limited purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept in an identifiable form for no longer than is necessary.
- Processed in a manner that ensures appropriate security.

5. Security of Personal Data

- We use appropriate technical and organizational measures to protect the personal data we collect and process. The measures we use are detailed in the Information security policy and are generally designed to provide a level of security appropriate to the risk of personal data that we process.
- Depending on requirements arising from business commitments or regulations, the following advanced technical solutions may be considered to provide an additional layer of protection:

  - Data Leak Prevention (DLP) tools: To monitor and restrict data flow from potential endpoints to unauthorized systems.
  - Data Masking: To restrict the ability to read sensitive data within the organization as well as to ensure protection from external parties.

6. Data Subject Rights

To adequately protect the personal data collected and processed by Fyxer AI, you must understand the rights to which data subjects are entitled. Listed below are the data subject rights that we adhere to:

- Right to be informed: The right to know how personal data is used in clear and transparent language.
- Right of access: The right to know and have access to the personal data held about an individual.
- Right to data portability: The right to receive and transfer data in a common and machine-readable electronic format.
- Right to be forgotten: The right to have personal data erased.
- Right to rectification: The right to have data corrected where it is inaccurate or incomplete.
- Right to object: The right to complain and to object to processing.
- Right to restriction of processing: The right to limit the extent of the processing of personal data according to an individual's wishes.
- Rights related to automated decision-making and profiling: The right not to be subject to decisions without human involvement.
- Right to non-discrimination: The right to not be discriminated against for an individual exercising their rights.

7. Staff Training

Fyxer AI ensures that its employees receive and attend the required data protection training, including the content and handling of this Policy, if they have constant or frequent access to personal data, are involved in the collection of data, or in the development of tools used to process personal data. The requirements of data protection and compliance must be observed. All Fyxer AI staff members need to annually acknowledge that they have attended the Data-Protection training and understand the Data Protection Policy.

8. Data Protection Officer

The Data Protection Officer leads all the data protection efforts of the company. The responsibilities of the Information Security Officer are detailed in the Information Security Policy.

9. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

10. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

11. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

12. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Data Protection Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Richard Hollingsworth	02 Jul, 2024
1	New Policy version Created	02 Jul, 2024