REED
SOCIETE GENERALE GROUP

GDPR Compliance Policy for Reed Management SAS

Date: Friday 6 September 2024
Reviewed by: Béatrice Causse
Approved by: Julien Touati

Table of Contents

1. Introduction

Reed Management SAS is committed to protecting the personal data of its investors, employees, and other stakeholders in compliance with the General Data Protection Regulation (GDPR). This policy outlines the Fund's approach to data protection, ensuring that personal data is processed lawfully, fairly, and transparently.

The GDPR applies to the processing of personal data within the European Union (EU) and to entities outside the EU that process the personal data of EU residents. As a private equity fund, we recognize the importance of safeguarding personal data throughout our operations, including during investment due diligence, portfolio management, and reporting.

2. Scope

This policy applies to all personal data processed by Reed Management SAS, including data related to:

- Investors (Limited Partners)
- Portfolio companies
- Employees and contractors
- Business partners and service providers

It covers all forms of data processing, including collection, storage, use, transfer, and disposal, whether electronic or paper-based.

3. Definitions

Key definitions under the GDPR include:

- Personal Data: Any information relating to an identified or identifiable natural person.
- Data Subject: The individual whose personal data is being processed.
- Processing: Any operation or set of operations performed on personal data, such as collection, storage, use, or destruction.
- Data Controller: The entity that determines the purposes and means of processing personal data (e.g., the Fund).
- Data Processor: The entity that processes personal data on behalf of the Data Controller.

4. Data Protection Principles

Reed Management SAS adheres to the following GDPR data protection principles:

- Lawfulness, Fairness, and Transparency: Personal data is processed lawfully, fairly, and in a transparent manner.
- Purpose Limitation: Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Data Minimization: Only the data necessary for the specified purpose is collected and processed.
- Accuracy: Personal data is kept accurate and up-to-date.
- Storage Limitation: Data is kept in a form that permits identification of data subjects for no longer than necessary.
- Integrity and Confidentiality: Personal data is processed in a manner that ensures security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- Accountability: The Fund is responsible for, and must be able to demonstrate, compliance with the GDPR.

5. Lawful Basis for Data Processing

The Reed Management SAS processes personal data based on one or more of the following lawful grounds:

- Consent: The data subject has given clear consent for the processing of their data for a specific purpose.
- Contractual Necessity: Processing is necessary for the performance of a contract with the data subject or to take steps at the data subject's request before entering into a contract.
- Legal Obligation: Processing is necessary to comply with a legal obligation.
- Legitimate Interests: Processing is necessary for the purposes of the legitimate interests pursued by the Fund, provided these interests are not overridden by the data subject's rights and interests.

The company carefully assesses the appropriate legal basis for each data processing activity and documents the justification.

6. Data Subject Rights

The company recognizes and respects the rights of data subjects under the GDPR. These rights include:

- Right to Access: Data subjects have the right to access their personal data and obtain information about how it is being processed.
- Right to Rectification: Data subjects can request correction of inaccurate or incomplete data.
- Right to Erasure (Right to be Forgotten): Data subjects can request deletion of their data in certain circumstances.
- Right to Restrict Processing: Data subjects can request a temporary halt to processing if they contest the accuracy of the data or object to the processing.
- Right to Data Portability: Data subjects can request their data in a structured, commonly used format and transfer it to another controller.
- Right to Object: Data subjects can object to the processing of their data, particularly when processing is based on legitimate interests or for direct marketing purposes.
- Rights Related to Automated Decision-Making: Data subjects have the right to not be subject to decisions based solely on automated processing, including profiling.

The Company has established procedures to handle and respond to data subject requests within the required timeframes.

7. Data Collection and Usage

Data Minimization

The Company only collects personal data that is necessary for legitimate business purposes, such as investor relations, regulatory compliance, and portfolio management. The Company avoids collecting excessive or irrelevant data and ensures that data is collected from reliable sources.

Data Storage and Retention

Personal data is stored securely and retained for no longer than necessary. The Company implements a data retention schedule that specifies the retention period for different categories of data, taking into account legal, regulatory, and operational requirements.

After the retention period, personal data is securely deleted or anonymized.

8. Data Sharing and Transfers

Third-Party Processors

The company may engage third-party service providers to process personal data on its behalf. In such cases, the Fund ensures that:

- A data processing agreement is in place, outlining the processor's responsibilities and compliance with GDPR.
- The third-party processor provides adequate security measures to protect personal data.

International Data Transfers

If the Company transfers personal data outside the European Economic Area (EEA), it ensures that adequate safeguards are in place, such as:

- Transfer to countries recognized by the European Commission as providing adequate protection.
- Use of Standard Contractual Clauses (SCCs) approved by the European Commission
- Implementing Binding Corporate Rules (BCRs) for intra-group transfers.
- The Fund assesses the risks associated with international data transfers and takes necessary measures to protect the data.

9. Security Measures

The Company implements appropriate technical and organizational measures to ensure the security of personal data. These measures include:

- Access Control: Limiting access to personal data to authorized personnel only.
- Encryption: Protecting data during transmission and storage through encryption technologies.
- Data Anonymization: Where possible, anonymizing or pseudonymizing personal data to minimize risks.
- Regular Security Audits: Conducting periodic security assessments to identify vulnerabilities and improve data protection measures.
- Incident Response Plan: Developing a response plan to handle security incidents and data breaches effectively.

10. Data Breach Management

The company has established procedures for identifying, reporting, and managing data breaches. Key components include:

- Breach Identification: Immediate identification of potential data breaches.

- Notification Obligations: If a breach is likely to result in a high risk to data subjects, the Fund will notify the relevant supervisory authority within 72 hours and inform affected data subjects without undue delay.
- Investigation and Mitigation: Prompt investigation of the breach to determine its scope, impact, and necessary corrective actions.

The company maintains a breach log to document all data breaches, regardless of severity.

11. Training and Awareness

The company provides regular GDPR training and awareness programs for all employees and contractors. Training covers:

- Data protection principles and compliance requirements
- Responsibilities under the GDPR
- Data breach reporting and response procedures
- Best practices for data security

The Fund ensures that all team members understand their role in protecting personal data and maintaining compliance with the GDPR.

12. Record Keeping and Documentation

The company maintains comprehensive records of its data processing activities, including:

- Data processing registers
- Data protection impact assessments (DPIAs) for high-risk processing activities
- Data subject consent records
- Data breach logs
- Records of third-party processing agreements

These records are regularly reviewed and updated to ensure ongoing compliance with GDPR requirements.

13. Compliance Monitoring and Review

The company regularly monitors its compliance with the GDPR and this policy. This includes:

- Internal Audits: Periodic audits to assess the effectiveness of data protection measures and identify areas for improvement.
- Policy Review: Annual review of the GDPR compliance policy to ensure it remains up-to-date with regulatory changes and best practices.
- External Audits: Engaging external auditors, where necessary, to provide independent assurance of compliance.

The company is committed to continuous improvement in its data protection practices and ensures that corrective actions are implemented promptly when compliance issues are identified.

14. Conclusion

The company is dedicated to ensuring full compliance with the GDPR and safeguarding the personal data of all individuals involved in its operations. By adhering to this policy, the Fund aims to maintain the trust of its investors, employees, and partners while minimizing the risks associated with data protection.