Compliance Documentation

Developed by Shield Wall IT for Valhalla Systems

Table of Contents

---

1. Purpose

The purpose of this SOP is to establish a process for developing and maintaining compliance documentation to demonstrate that Valhalla Systems meets the requirements of the General Data Protection Regulation (GDPR).

---

2. Scope

This SOP applies to all systems, processes, and personnel involved in handling, processing, and storing personal data of individuals within the European Union (EU) at Valhalla Systems.

---

3. Responsibilities

- **Compliance Officer:** Responsible for overseeing compliance efforts and ensuring documentation is accurate and up to date.
- **IT Security Team:** Responsible for implementing and maintaining security controls as per GDPR requirements.
- **System Administrators:** Ensure that systems are configured and maintained in compliance with GDPR standards.
- **Employees and Contractors:** Must adhere to compliance policies and report any non-compliance issues.

4. GDPR Compliance Documentation

Documentation Requirements

1. **Policies and Procedures:**
    - Develop and maintain data protection policies and procedures that address GDPR requirements.
    - Ensure that all employees are aware of and follow these policies.
2. **Data Inventory:**
    - Document all personal data processed by the organization, including the purpose of processing, data subjects involved, and data flows.
3. **Records of Processing Activities (ROPA):**
    - Maintain detailed records of processing activities, including categories of data subjects, categories of personal data, processing purposes, and data retention periods.

Data Protection Measures

1. **Data Protection by Design and Default:**
    - Implement technical and organizational measures to ensure data protection principles are embedded into processing activities from the outset.
    - Document the measures taken to achieve data protection by design and default.
2. **Data Security:**
    - Ensure that personal data is encrypted at rest and in transit.
    - Document the encryption methods and key management practices used.

Access Control

1. **Access Management:**
    - Document procedures for assigning and managing access to personal data.
    - Ensure that access is granted on a need-to-know basis and is regularly reviewed.
2. **Authentication:**
    - Implement and document multi-factor authentication for accessing systems that handle personal data.

Data Subject Rights

1. **Right to Access:**
    - Document procedures for responding to data subject access requests (DSARs).
    - Ensure data subjects can obtain information about their personal data processing.
2. **Right to Rectification:**
    - Document procedures for correcting inaccurate or incomplete personal data upon request.
3. **Right to Erasure:**

    - Document procedures for deleting personal data upon request, under certain conditions.
4. **Right to Restrict Processing:**
    - Document procedures for restricting the processing of personal data upon request, under certain conditions.
5. **Right to Data Portability:**
    - Document procedures for providing data subjects with their personal data in a commonly used format.
6. **Right to Object:**
    - Document procedures for handling objections to the processing of personal data for certain purposes.

Incident Response Plan

1. **Incident Response Procedures:**
    - Develop and document an incident response plan that addresses GDPR requirements for data breach notification.
    - Ensure that all employees are trained on incident response procedures and know their roles in the event of a data breach.
2. **Data Breach Notification:**
    - Document procedures for notifying the relevant supervisory authority within 72 hours of becoming aware of a data breach.
    - Document procedures for notifying affected data subjects when required.

---

5. Review and Revision

This SOP will be reviewed annually or as needed based on changes in GDPR requirements or organizational needs. All revisions will be documented in the revision history section below.

Revision History

Date	Version	Description	Author
5/28/2024	1.0	Initial Version	Gilbert Collado

Approval: I have read and understand the terms and conditions of this Compliance Documentation SOP.

Employee Name (Print): _____

Employee Signature: _____

Date: _____