Procedure for handling members' personal data (test document)

Purpose

The purpose of this procedure is to establish guidelines for the Chapter Manager of EO to ensure that all personal data of members is handled in compliance with applicable data protection laws and EO’s privacy policies. The procedure aims to protect the confidentiality, integrity, and availability of member data and to outline the responsibilities and best practices for managing such information.

Scope

This procedure applies to the EO Chapter Manager and any individual or third party acting on behalf of the EO chapter. It covers all activities related to the collection, storage, use, sharing, and disposal of personal data belonging to EO members.

Definitions

- **Personal Data**: Any information that can be used to identify a person directly or indirectly, such as name, email address, phone number, business information, or any other data specific to an individual.
- **Sensitive Data**: Data that includes information such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health data, or any other information that is considered sensitive under data protection laws.
- **Data Subject**: The individual (EO member) whose personal data is being processed.

- **Processing**: Any operation performed on personal data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, erasure, or destruction.

Roles and Responsibilities

- **Chapter Manager**: Responsible for ensuring compliance with this procedure, managing access to personal data, and reporting any data breaches or non-compliance issues to the Global EO Data Protection Officer.
- **EO Leadership Team**: Supports the Chapter Manager in implementing data protection measures and responding to data subject requests.
- **Global EO Data Protection Officer (DPO)**: Provides guidance on data protection issues, monitors compliance, and addresses any escalated concerns related to personal data.

Data Collection and Use

1. **Data Collection**:
   - Collect only the data necessary for EO chapter operations, such as member registration, event coordination, and communication purposes.
   - When collecting data, ensure that members are informed about the purpose of data collection, how it will be used, and obtain their explicit consent where required.
   - Use standardized EO data collection forms (e.g., registration, consent forms) to ensure consistency and compliance.
2. **Data Storage**:
   - Store personal data in secure, password-protected systems, such as EO’s official CRM tools or authorized cloud storage services.
   - Physical documents containing personal data (e.g., printed membership applications) must be stored in a locked cabinet in the chapter office.
   - Ensure that access to data is restricted to authorized personnel only, based on the principle of least privilege.
3. **Data Use**:
   - Use personal data only for the purposes for which it was collected (e.g., event management, membership communication).
   - Do not use or share personal data for marketing or third-party activities without explicit consent from the member.

Access Management

1. **Granting Access**:
   - Access to member data is granted only to individuals who require it to perform their official duties.
   - Use role-based access control (RBAC) to define and limit data access permissions.
2. **Review and Revocation**:
   - Regularly review access permissions and remove access for individuals who no longer need it (e.g., former chapter employees or volunteers).
   - Implement an offboarding process for Chapter Managers and other staff members that includes revoking access to all EO systems containing personal data.

Data Sharing and Disclosure

1. **Internal Sharing**:
   - Share member data internally only on a need-to-know basis and ensure that the recipient understands their obligations to protect the data.
2. **External Sharing**:
   - Do not share personal data with external parties (e.g., service providers, partners) without a Data Processing Agreement (DPA) in place.
   - Before sharing, verify that the external party meets EO’s data protection standards.
3. **Event Coordination**:
   - For event coordination, share only the minimum necessary data (e.g., dietary preferences, emergency contact information) and ensure that the data is securely handled by all parties involved.

Data Retention and Disposal

1. **Data Retention**:
   - Retain personal data only for as long as it is needed for operational purposes or as required by law.
   - Conduct regular reviews of stored data and remove any outdated or unnecessary information.
2. **Data Disposal**:
   - When disposing of personal data, ensure that it is permanently and securely deleted (e.g., shredding physical documents, using secure deletion tools for digital data).
   - Maintain a record of disposed data, including the type of data, date of disposal, and method used.

Data Breach Response

1. **Definition of Data Breach**:
   - A data breach is any unauthorized access, disclosure, alteration, or destruction of personal data.
2. **Immediate Response**:
   - Upon discovering a data breach, notify the EO Global Data Protection Officer within 24 hours.
   - Document all details of the breach, including the type of data involved, the cause of the breach, and the actions taken to mitigate it.
3. **Member Notification**:
   - If the data breach poses a high risk to the rights and freedoms of affected members, promptly notify them with information on what data was affected and recommended steps for protection.

Data Subject Rights

1. **Right to Access**:
   - Members have the right to request access to their personal data and to know how it is being used.
   - Respond to such requests within 30 days and provide a copy of the data upon verification of the requester’s identity.
2. **Right to Rectification**:
   - Members have the right to request corrections to inaccurate or incomplete data.
   - Make the necessary corrections within 30 days and inform the member once completed.
3. **Right to Erasure (Right to be Forgotten)**:
   - Members can request the deletion of their data under specific conditions (e.g., withdrawal of consent, data no longer needed).
   - Review and process these requests in accordance with EO’s data retention policy.

Training and Awareness

1. **Training for Chapter Manager**:
   - Complete annual training on data protection and privacy best practices.
   - Stay updated on changes to data protection regulations and EO’s privacy policies.
2. **Member Awareness**:

- Regularly inform members of their data protection rights and how EO is handling their personal information.

Monitoring and Compliance

1. **Internal Audits**:
   - Conduct annual internal audits to assess compliance with this procedure and identify areas for improvement.
2. **Corrective Actions**:
   - Address any identified compliance issues promptly and implement corrective actions to prevent recurrence.

Revision #3
Created 27 September 2024 08:27:57 by Admin
Updated 5 November 2024 14:50:14 by Admin