THE FRANK SOO FOUNDATION

GDPR Audit Checklist

The Frank Soo Foundation is committed to upholding the highest standards of data protection, it is crucial to regularly audit our compliance with the General Data Protection Regulation (GDPR) and associated UK data protection laws. This checklist serves as a comprehensive guide to ensure we adhere to the requirements set forth by the Information Commissioner's Office and maintain our duty of care towards personal data.

1. Data Inventory

- **Identify Data Holdings**: List all personal data held by the charity, including donor information, beneficiary details, employee records, and volunteer data.
- **Categorise Data**: Classify the data according to its sensitivity, including special categories of personal data as defined by GDPR (e.g., health information, racial or ethnic origin).

2. Purpose of Data Processing

- **Document Processing Purposes**: Clearly outline the purposes for which personal data is processed.
- **Review Lawful Basis for Processing**: Confirm that each processing activity is supported by a lawful basis under Article 6 of GDPR: consent, contract, legal obligation, vital interests, public task, or legitimate interests.

3. Consent Management

- **Consent Review**: Assess whether consent obtained from data subjects is explicit, informed, and unambiguous.
- **Maintain Consent Records**: Ensure there are clear records of consent, including what data was collected, why it was collected, and how consent was obtained.

4. Data Subject Rights

- **Access Requests**: Implement and review procedures for handling data subject access requests (DSARs) within the one-month response timeframe.
- **Right to Rectification and Erasure**: Ensure appropriate mechanisms are in place for data subjects to request corrections or deletion of their data, in compliance with GDPR.

5. Data Processing Agreements

- **Review Third-Party Contracts**: Verify that any third parties processing personal data on behalf of the charity have appropriate Data Processing Agreements (DPA) in place.
- **Assess Sub-Processors**: Ensure that any sub-processors are also compliant with GDPR requirements.

6. Data Security Measures

- **Assess Technical and Organisational Measures**: Evaluate current data security measures to protect personal data against unauthorised access, loss, or destruction.
- **Implement Staff Training**: Provide regular training to staff on data protection policies and procedures to mitigate risks associated with data handling.

7. Data Breach Response Plan

- **Establish Breach Protocol**: Confirm that there is a clear plan in place for identifying and managing data breaches.
- **Notification Procedures**: Ensure that procedures are in place to notify the Information Commissioner's Office and affected data subjects in the event of a reportable breach.

8. Privacy Notices

- **Review Privacy Policies**: Ensure that privacy notices are clear, concise, and accessible, providing all required information to data subjects as stipulated by GDPR.
- **Regular Updates**: Maintain a schedule for reviewing and updating privacy notices in alignment with changes to data processing practices.

9. Record Keeping

- **Maintain Records of Processing Activities**: Document all processing activities in accordance with Article 30 of GDPR.
- **Audit Trail**: Ensure that there is a comprehensive audit trail for data handling activities to demonstrate accountability.

10. Data Protection Impact Assessments (DPIAs)

- **Conduct DPIAs**: Identify situations where a DPIA is required and carry out assessments to evaluate risks and implement mitigation measures.
- **Review Outcomes**: Regularly review the outcomes and effectiveness of DPIAs conducted.

11. Data Transfers

- **Evaluate Data Transfers**: Identify any transfers of personal data outside the UK or the European Economic Area (EEA) and ensure compliance with GDPR provisions.
- **Assess Safeguards**: Verify that adequate safeguards, such as standard contractual clauses or adequacy decisions, are in place for international data transfers.

12. Appoint a Data Protection Officer (DPO)

- **Designate a DPO**: If required, appoint a qualified individual to oversee data protection compliance and act as a point of contact for data subjects and the ICO.
- **Ensure DPO Availability**: Make sure that the DPO is easily accessible and appropriately resourced to fulfil their responsibilities.

Conclusion

By adhering to this audit checklist, we can systematically assess our compliance with GDPR and ensure that we are protecting the personal data of our stakeholders effectively. Regular audits are essential to not only safeguard data but also to foster trust and transparency with our beneficiaries and supporters. As a charity, we are dedicated to upholding our ethical obligations and legal responsibilities in data protection.