



GDPR POLICY

Ark Of Hope Foundation For All Nations

Last Updated: April 2024

www.arkkofhopefoundation.com
info@arkkofhopefoundatiion.com

1. Introduction

Ark of Hope Foundation for All Nations ("Ark of Hope Foundation") is dedicated to protecting the privacy and rights of individuals in accordance with the General Data Protection Regulation (GDPR). This policy outlines our commitment to data protection principles and procedures to ensure compliance with GDPR requirements.

2. Commitment to Legal Principles

Ark of Hope Foundation adheres to the fundamental principles of GDPR, ensuring that all personal data is:

- Processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Retained only for as long as necessary for the purposes for which it was collected.
- Handled in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage.

3. Commitment to Data Subject Rights

Ark of Hope Foundation respects the rights of individuals regarding their personal data, including:

- The right to be informed about the collection and use of their personal data.
- The right of access to their personal data through Subject Access Requests (SARs).
- The right to rectification of inaccurate or incomplete personal data.
- The right to erasure of personal data ("right to be forgotten").
- The right to restrict processing of personal data.
- The right to data portability.
- The right to object to processing of personal data.
- Rights in relation to automated decision making and profiling.

4. Staff GDPR Training

Ark of Hope Foundation provides comprehensive GDPR training to all employees and volunteers involved in processing personal data. The training includes:

- GDPR Awareness: Understanding the key principles and requirements of GDPR.
- Roles and Responsibilities: Clarifying the responsibilities of staff in ensuring data protection compliance.
- Data Handling Procedures: Guidance on how to handle personal data securely, including data storage, access controls, and encryption.
- Data Breach Management: Procedures for recognising, reporting, and responding to data breaches. Full Data Breach Procedure has been provided in Appendix 1
- Subject Access Requests (SARs): Training on how to recognise and manage SARs effectively.

5. Procedures to Manage Subject Access Requests (SARs)

Ark of Hope Foundation acknowledges and upholds the rights of data subjects, including the right to access their personal data through SARs. The following procedures are implemented:

Receipt of SARs: SARs may be received verbally or in writing. Staff members receiving SARs should immediately forward them to the Data Protection Officer (DPO), **Stella King** through email: stella@artofhopefoundation.com

Verification of Identity: Before responding to a SAR, Ark of Hope Foundation verifies the identity of the data subject to prevent unauthorised disclosures.

Response Time: Ark of Hope Foundation aims to respond to SARs promptly and within the GDPR-mandated timeframe of one month. This period may be extended by two further months for complex or numerous requests, and the data subject will be informed of any extension and the reasons for it within one month of receipt of the request.

Format of Response: Responses to SARs are provided in a clear and understandable format, explaining the procedures for requesting a review of the response or making a complaint to the supervisory authority.

6. Data Security

Ark of Hope Foundation implements robust technical and organisational measures to ensure the security of personal data, including:

Access Controls: Limiting access to personal data to authorised personnel only.

Encryption: Encrypting personal data both in transit and at rest where appropriate.

Data Minimisation: Collecting only the personal data necessary for specified purposes.

Regular Audits: Conducting regular audits of data processing activities to identify and mitigate security risks.

7. Policy Review and Updates

This GDPR policy, along with related procedures, will be reviewed annually or as necessary to ensure compliance with changes in GDPR regulations and organisational practices. Updates will be communicated to all staff and stakeholders.

8. Related Policies and Procedures


Data Retention and Deletion Policy: Defines how long data is kept and the process for secure deletion.

IT and Security Policies: Includes acceptable use of IT, cybersecurity measures, and handling of sensitive data on personal devices.

Data Processing Procedures: Specifies lawful bases for data processing, procedures for different types of data, and collaboration with third parties.

9. Compliance and Enforcement

Ark of Hope Foundation ensures that all staff and volunteers understand their roles and responsibilities in complying with this GDPR policy and related procedures. Non-compliance may result in disciplinary action as outlined in the organisation's policies.



Appentix 1: Data Breach Procedure

In the event of a data breach involving personal data, Ark of Hope Foundation (AOH) will follow a comprehensive procedure to ensure compliance with GDPR and to mitigate adverse effects on individuals, the organisation, and its stakeholders. This procedure is crucial for detecting, investigating, risk-assessing, and recording any breaches, as well as reporting them as required. Effective processes are in place to manage such incidents, preventing serious repercussions like financial penalties, reputational damage, loss of business, and disciplinary action.

Detection and Management:

- **Training:** Staff are trained to recognise security incidents and personal data breaches.
- **Incident Management Team:** A dedicated team manages security incidents and breaches.
- **Reporting:** Staff promptly escalate security incidents to the appropriate team to determine if a breach has occurred. Systems are in place to facilitate the reporting of incidents and breaches.
- **Response Plan:** The organisation has a response plan for promptly addressing any security incidents and breaches.

Assessment and Containment:

- **Immediate Action:** Identify and contain the breach to prevent further unauthorised access or damage.
- **Risk Assessment:** Assess the likelihood and severity of the risk to individuals resulting from the breach.
- **Documentation:** Log and document all facts related to the breach, including causes, affected data, effects, and remedial actions.


Notification:

Supervisory Authority: Notify the relevant supervisory authority within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms.

Affected Individuals: Notify individuals without undue delay if the breach poses a high risk to their rights and freedoms. Provide clear, plain language information including:

- Description of the breach.
- Contact details of the Data Protection Officer (DPO).
- Likely consequences.
- Measures taken to address and mitigate the breach.
- Advice for individuals to protect themselves.

Investigation and Remediation:

- **Root Cause Analysis:** Conduct a detailed investigation to determine the root cause of the breach.
 - **Preventive Measures:** Implement measures to address the root cause and prevent future breaches.
 - **Policy Review:** Update policies and procedures as necessary to enhance data security.
- 

Review and Monitoring:

- **Trend Analysis:** Analyse breach reports to prevent recurrence. Monitor the type, volume, and cost of incidents, and conduct trend analysis over time.
- **Audit and Compliance:** Perform internal audits and engage external audits or compliance checks. Monitor staff adherence to data protection policies and procedures.
- **Performance Indicators:** Track KPIs regarding data protection compliance, information governance, security incidents, and training completion rates.

Accountability and Record Keeping:

- **Central Log:** Maintain a detailed record of breaches and near misses, documenting causes, what happened, affected data, effects, and remedial actions.
 - **Audit Plan:** Keep a central audit plan/schedule for data protection and information governance audits. Produce audit reports and action plans to address findings.
 - **Management Information:** Communicate outcomes of monitoring and review activities to relevant stakeholders, including senior management, to inform discussions and actions.
- 