THE KHALIFA IHLER INSTITUTE
WWW.KHALIFAIHLER.ORG

Data Protection Policy

Khalifa Ihler Institute

Last updated	09/03/2021

Definitions

DPO	Data Protection Officer, (responsible person), David Cerenzia, (david@khalifaihler.org)
GDPR	General Data Protection Regulation
KII	Acronym for, Khalifa Ihler Institute
Register of Systems	A register of all systems or contexts in which personal data is processed by KII
User	Person who
Volunteer	Person acting in voluntary capacity with KII

---

1. **Data Protection Principles**

The **Khalifa Ihler Institute** is committed to processing and retaining data in accordance with our responsibilities under the **General Data Protection Regulation 2016/679**

Article 5 of the **GDPR** requires that personal data shall be:

a) Processed lawfully, fairly, and in a transparent manner in relation to individuals;

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with initial purposes;
c) adequate , relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to purposes for which they are processed, are erased or rectified without delay'
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for no longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

---

2. **General Provisions**
   a) This policy applies to all personal data processes by KII.
   b) The DPO shall take responsibility for KII's ongoing compliance with this policy.
   c) This policy shall be reviewed annually.

d) KII shall register with the Information Commissioner's Office as an organisation that processes personal data.

---

3. **Lawful, fair and transparent processing**
   a) To ensure its processing of data is lawful, fair and transparent, our association shall maintain an internal Register of Systems.
   b) The Register of Systems shall be reviewed at least annually.
   c) Individuals have the right to access their personal data and any such requests made to KII shall be dealt with in a timely manner.

---

4. Lawful purposes
   a) All data processed by KII must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
   b) KII shall note the appropriate lawful basis in the Register of Systems.
   c) Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
   d) Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be inplace to ensure such revocation is reflected accurately in KII's systems.

---

5. Data minimisation
   a) KII shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to purposes for which they are processed.

---

6. Accuracy

a) KII shall take reasonable steps to ensure personal data is accurate.
b) Where necessary for a lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

---

7. Archiving / Removal

a) To ensure that personal data is kept for no longer than necessary, KII shall put in place archiving policy for each area in which personal data is processed and review this process annually.
b) The archiving policy shall consider what data should/must be retained, for how long and why.

---

8. Storage and security

a) KII will use Airtable, (primary storage), and Google Work Space, (secondary storage), for collected data
    i. **Air Table**
        - Air Table utilises 256-bit TLS encryption to protect transmission of data between users, (KII), and Air Table servers
        - While data is at rest, it is further encrypted by Airtable with AES-256
        - Air Table servers have received SOC 1, SOC 2, and ISO/IEC 27001 security management certifications, and uphold industry best practices.
    ii. **Google Work Space**

- Under Google's Data Processing Amendment, authority is placed in the customer, (KII), to act as the controller of the data stored on Google Drive.
- KII is the soul party who can determine the measures and purposes of how data stored is processed.
- Google Work Space has received the ISO/ IEC 27001 security management certification, and uphold industry best practices

b) KII shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
c) Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
d) When personal data is deleted this should be done safely such that the data is irrecoverable.
e) Appropriate back-up and disaster recovery solutions shall be in place.

---

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, KII shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Swedish Authority for Privacy Protection.