GO GLOBAL Scaling Up Romanian Tech Startups Globally

DATA PROTECTION POLICY

1. PURPOSE, SCOPE & USERS

Asociația Pro Digitalizare și Etica în Tehnologie, hereinafter referred to as the "NGO," strives to comply with applicable laws and regulations related to personal data protection in countries where the NGO operates. This Policy sets forth the basic principles by which the NGO processes the personal data of participants, sponsors, partners, business collaborators, employees, and other individuals, and indicates the responsibilities of its departments and employees while processing personal data.

This Policy applies to the NGO and its directly or indirectly controlled entities conducting activities within the European Economic Area (EEA) or processing the personal data of data subjects within the EEA.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of the NGO.

2. DEFINITIONS

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation (GDPR):

- **Personal Data**: Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or an online identifier.
- **Sensitive Personal Data**: Personal data that are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and merit specific protection. Such data include racial or ethnic origin, political opinions, religious beliefs, or data concerning a person's health or sexual orientation.
- **Data Controller**: The natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Data Processor**: A natural or legal person, public authority, agency, or other body that processes personal data on behalf of a Data Controller.
- **Processing**: Any operation or set of operations performed on personal data, such as collection, recording, organization, structuring, storage, adaptation, retrieval, or destruction.

3. BASIC PRINCIPLES REGARDING PERSONAL DATA PROCESSING

The data protection principles outline the basic responsibilities for organizations handling personal data. Article 5(2) of the GDPR stipulates that the "controller shall be responsible for, and be able to demonstrate, compliance with the principles."

- **Lawfulness, Fairness & Transparency**: Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose Limitation**: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- **Data Minimization**: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy**: Personal data must be accurate and, where necessary, kept up to date. Inaccurate data must be erased or rectified promptly.
- **Storage Period Limitation**: Personal data must not be kept for longer than is necessary for the purposes for which they are processed.
- **Integrity & Confidentiality**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- **Accountability**: The NGO must be able to demonstrate compliance with these principles.

4. DATA COLLECTION & PROCESSING

The NGO collects personal data voluntarily provided by individuals interested in participating in the tech startup scaling program or becoming sponsors/partners. Personal data collected may include:

- Name
- Email address
- Company name (for sponsors or partners)
- Other relevant information provided voluntarily

The NGO processes this data solely for the purpose of managing applications, communication with participants, sponsors, and partners, and for facilitating participation in the program.

5. DISCLOSURE TO THIRD PARTIES

The NGO may share personal data with third-party partners or sponsors directly involved in the program's execution. These third parties will only process the data for purposes related to the program and in accordance with applicable data protection laws.

6. CROSS-BORDER TRANSFER OF PERSONAL DATA

Any transfer of personal data outside the European Economic Area (EEA) will be done only with appropriate safeguards in place and in compliance with GDPR requirements.

7. RIGHTS OF DATA SUBJECTS

Data subjects have the following rights with respect to their personal data:

- **Access**: Right to request access to their data.
- **Rectification**: Right to request correction of inaccurate data.
- **Erasure**: Right to request deletion of their data (“right to be forgotten”).
- **Restriction of Processing**: Right to restrict the processing of their data.
- **Data Portability**: Right to receive their data in a structured, commonly used format.

- **Objection**: Right to object to the processing of their data.

8. DATA PROTECTION OFFICER (DPO)

The NGO has appointed a Data Protection Officer responsible for overseeing data protection strategy and ensuring compliance with GDPR.

Contact:

For any questions or requests regarding personal data, you can contact us at:
Email: **team@upgrade100.com**

9. LEAD SUPERVISORY AUTHORITY

The lead supervisory authority for the NGO is the Romanian Data Processing Authority:
Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
B-dul G-ral. Gheorghe Magheru 28-30
Sector 1, cod postal 010336, București, Romania
Email: anspdcp@dataprotection.ro

10. RESPONSE TO PERSONAL DATA BREACH INCIDENTS

In the event of a personal data breach, the NGO will notify the relevant authorities within 72 hours if the breach poses a risk to the rights and freedoms of data subjects.

11. AUDIT & ACCOUNTABILITY

The NGO is responsible for auditing the implementation of this Policy to ensure ongoing compliance. Any violation of this Policy may lead to disciplinary measures.

12. CONFLICTS OF LAW

In the event of any conflict between this Policy and applicable laws, the latter shall prevail.