FOUNDATION "INSTITUTE OF HUMAN RIGHTS AND MEDIA" (IPCIM)

Personal Data Protection Policy (GDPR)

§ 1. General Provisions and Scope

1. This Policy establishes the principles and procedures for personal data processing and protection (GDPR) within the Foundation "Institute of Human Rights and Media" (IPCIM).
2. The Foundation acts as the Personal Data Controller within the meaning of Article 4 of the GDPR.
3. This Policy applies to all governing body members, employees, associates, and volunteers who have access to personal data.

§ 2. Fundamental GDPR Principles

1. Data shall be processed lawfully, fairly, and in a transparent manner.
2. Data shall be collected for specified, explicit, and legitimate purposes.
3. Data processing shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
4. The Foundation shall ensure data accuracy and currency, and store data in a form permitting identification of data subjects for no longer than is necessary.

§ 3. Data Protection Governance

1. The Foundation shall designate a person responsible for GDPR oversight (Data Protection Officer – DPO, or another individual designated by the Management Board).
2. The Foundation maintains a Record of Processing Activities (ROPA), documenting the purpose, scope, and legal basis of processing for every processing activity.
3. All employees and associates of the Foundation are required to sign an AUTHORISATION to process personal data as well as a Non-Disclosure Commitment.

§ 4. Security Measures and Breach Notification Procedure

1. **Technical Measures:** The Foundation implements technical safeguards (e.g., encryption, strong passwords, firewalls, regular system updates, and periodic backups) to protect personal data against unauthorised access, loss, destruction, or damage.
2. **Data Breach Notification Procedure:**
    1. Every employee/associate must immediately report any suspected data breach (e.g., loss of a laptop, password leak, accidental email delivery) to the Management Board.
    2. The Management Board/DPO is obligated to notify the President of the Personal Data Protection Office (PUODO) within 72 hours of becoming aware of the breach, provided that the breach is likely to result in a risk to the rights and freedoms of natural persons.

3. Data subjects shall be informed of the breach if it is likely to result in a high risk to their rights and freedoms.

§ 5. Rights of Data Subjects

1. The Foundation facilitates the exercise of data subjects' rights (Data Subject Rights):
    1. Right of access by the data subject.
    2. Right to rectification and completion of data.
    3. Right to erasure ("right to be forgotten").
    4. Right to restriction of processing.
    5. Right to data portability (where applicable).
    6. Right to object to data processing.
2. Requests concerning the exercise of rights shall be handled within 30 days.

§ 6. Final Provisions

1. This Policy enters into force on the date of its adoption by the Management Board of the Foundation and is subject to mandatory review no less than once every two years.