

FOUNDATION "INSTITUTE OF HUMAN RIGHTS AND MEDIA"

GDPR ANNEX – PERSONAL DATA MANAGEMENT SYSTEM

RECORD OF PROCESSING ACTIVITIES (ROPA)

Compliant with Art. 30(1) of the GDPR and the GDPR Policy of IPCIM

Data Controller (DC): Foundation "Institute of Human Rights and Media" with its registered seat in Warsaw

Body Acting on Behalf of DC: Management Board of the IPCIM Foundation | **Contact:** kontakt@ipcim.org

DPO Status: Data Protection Officer (DPO) has not been appointed within the Foundation structure (direct responsibility of the Management Board).

No.	Name of Activity / Process	Purpose of Processing	Data Subjects	Categories of Data	Legal Basis	Data Recipients	Retention Period	Security Measures
1.	Recruitment and Personnel Employment	Conclusion and performance of employment / civil law contracts, HR and payroll services	Employees, contractors, job applicants	First name, surname, PESEL (tax/national ID), address, bank account no., education, employment history	Art. 6(1)(b) & (c) GDPR (Labor Code)	Accounting firm, ZUS (Social Insurance), Tax Office, HR software providers	5 years from end of year (contracts) / personnel file retention up to 10/50 years	Password-protected file encryption, key-restricted access
2.	Handling Inquiries and Contact	Conducting correspondence, handling complaints, requests, and security alerts	Beneficiaries, reporting individuals, contacting individuals	First name, surname, e-mail address, phone number, message content	Art. 6(1)(f) GDPR (Legitimate Interest)	Email service providers, hosting provider	Case resolution + 3 years (statute of limitations)	Email encryption (TLS/SSL), system authentication
3.	Database of Experts and Volunteers	Appointing expert committees, participation in research and statutory projects	Independent experts, volunteers, interns	First name, surname, academic title, field of expertise, e-mail, phone, bank account no.	Art. 6(1)(b) & (a) GDPR (Consent / Contract)	Foundation bodies, project partners	Until withdrawal of consent / end of cooperation + 5 years	Access restriction, system authorization levels
4.	Whistleblower Handling	Receiving and verifying reports of legal violations	Whistleblowers, individuals named in notifications	Identification data, contact details, content of the report	Art. 6(1)(c) GDPR (Whistleblower Protection Act)	Authorized Management Board of IPCIM, law enforcement authorities	3 years following the end of the calendar year in which the	Dedicated encrypted channel, anonymization

No.	Name of Activity / Process	Purpose of Processing	Data Subjects	Categories of Data	Legal Basis	Data Recipients	Retention Period	Security Measures
							report was resolved	

FOUNDATION "INSTITUTE OF HUMAN RIGHTS AND MEDIA"

PERSONAL DATA PROTECTION SYSTEM DOCUMENTATION (GDPR)

AUTHORIZATION TO PROCESS PERSONAL DATA

Authorization Number: UPO / _____ / _____

Acting on behalf of the Personal Data Controller – the Management Board of the Foundation "Institute of Human Rights and Media" with its registered seat in Warsaw (IPCIM), pursuant to Article 29 of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and the Personal Data Protection Policy of IPCIM:

I hereby authorize Mr./Ms.:

Full Name: _____

Position / Role in IPCIM: _____

PESEL Number / ID: _____

to process personal data within the areas and data sets managed by the IPCIM Foundation, to the extent necessary to perform official duties or carry out tasks under the cooperation agreement.

1. Scope of Authorization

The authorization includes the following operations on personal data (please mark as applicable):

- ☐ Viewing and reading data
- ☐ Entering, modifying, and editing data
- ☐ Deleting and archiving data
- ☐ Managing Foundation IT systems (email, databases, cloud storage)

2. Duration of Authorization

This authorization is valid from _____ until:

- ☐ Expiration or termination of employment / cooperation contract with the IPCIM Foundation
- ☐ Revocation of authorization by the Management Board of the Foundation

3. Duties of the Authorized Person

The authorized person is strictly required to:

1. Process personal data exclusively in accordance with the instructions of the Foundation Management Board and the implemented IPCIM GDPR Policy;
2. Maintain the confidentiality of processed personal data and security measures;
3. Protect data against unauthorized access, loss, modification, or damage;
4. Immediately report any suspected personal data protection breach to the Management Board of IPCIM.

Signature of President / Board Member of IPCIM

CONFIRMATION OF RECEIPT OF AUTHORIZATION

I declare that I have received this authorization, read the Personal Data Protection Policy of the IPCIM Foundation, and undertake to strictly comply with it.

Date: _____

Legible signature of the authorized person

IPCIM Foundation – Personal Data Protection Documentation | Page 2-3 of 5

FOUNDATION "INSTITUTE OF HUMAN RIGHTS AND MEDIA"

INFORMATION SECURITY AND GDPR DOCUMENTATION

NON-DISCLOSURE STATEMENT

Template for IPCIM Employees, Experts, and Associates

I, the undersigned:

Full Name: _____

PESEL / Identity Document No.: _____

Role in IPCIM (e.g., Employee, Expert, Committee Member): _____

In connection with the performance of duties or execution of cooperation for the benefit of the Foundation "Institute of Human Rights and Media" (IPCIM) with its registered seat in Warsaw, I hereby declare and undertake to comply with the following principles:

1. Scope of Confidentiality

I undertake to keep in strict confidence all confidential information, legally protected information, personal data, and organizational secrets of the IPCIM Foundation to which I gain access during the performance of my duties or cooperation.

2. Definition of Confidential Information

Confidential Information includes, in particular:

- All personal data processed in the databases and systems of the IPCIM Foundation;
- Data regarding research projects, expert assessments, unpublished reports, legal opinions, internal procedures, and operational strategies of IPCIM;
- Organizational, financial, technical, and legal information regarding the Foundation and its partners, grantors, and beneficiaries.

3. Specific Obligations

I undertake to:

1. Not use Confidential Information for purposes other than the proper performance of my tasks for the Foundation;
2. Not disclose, make available, or transfer Confidential Information to third parties without the explicit, written consent of the Management Board of the IPCIM Foundation;
3. Comply with the information security procedures and GDPR regulations implemented within the Foundation.

4. Duration of Obligation

The non-disclosure obligation remains effective during the term of my employment/cooperation with the IPCIM Foundation, as well as after its termination, without time limitation.

5. Liability for Breach

I acknowledge that a breach of this statement may result in:

- Immediate termination of employment / contract for cause (disciplinary grounds);
- Civil liability for damages caused to the IPCIM Foundation;
- Criminal liability arising under applicable legal regulations (including the Personal Data Protection Act and the Penal Code).

City and Date: _____

Legible signature of the declarant

IPCIM Foundation – Personal Data Protection Documentation | Page 4-5 of 5