NGO «RUKH Global»

hello@rukh.global
www.rukh.global

Company ID: 46294025
Legal address: Ukraine, 08290,
Kyiv Region, Bucha District,
Hostomel, 12A Patriotiv St.

APPROVED
by the decision of the Management Board
of NGO "RUKH Global"
Minutes No. 3 dated "17" April 2026

Chairman of the Management Board
_____ Igor DUDKA

Executive Director
_____Maryna MAKHOTA

REGULATION

ON THE PROCESSING AND PROTECTION OF PERSONAL DATA

OF THE NON-GOVERNMENTAL ORGANIZATION "RUKH GLOBAL"

(GDPR Compliance — Regulation (EU) 2016/679 and Law of Ukraine No. 2297-VI)

Version: 1.0
Effective date: "17" April 2026
Next review: April 2028 (or upon change of legal basis / donor requirements)
Responsible for maintenance: Data Protection Officer (DPO)
Approved by: Management Board of NGO "RUKH Global"

1. GENERAL PROVISIONS

1.1. Purpose and Objectives of the Regulation

1.1.1. This Regulation on the Processing and Protection of Personal Data (hereinafter — the Regulation) defines the principles, rules, procedures, and measures adhered to by the Non-governmental organization "RUKH Global" (hereinafter — the Organization, RUKH Global, Controller) when processing personal data of natural persons (hereinafter — data subjects).

1.1.2. The objective of the Regulation is to ensure compliance with the requirements of:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, hereinafter — GDPR);
- Law of Ukraine "On Personal Data Protection" No. 2297-VI of 01 June 2010 (hereinafter — Law No. 2297-VI);
- Other regulatory and legal acts of Ukraine and the EU in the sphere of personal data protection;
- Requirements of the Organization's donors (EU, UN agencies, GIZ, SIDA) concerning the protection of personal data of beneficiaries, partners, and employees.

1.1.3. The Regulation is adopted in implementation of Clause 3.2.7 of the Charter of NGO "RUKH Global", which stipulates that the Organization processes and protects personal data of members, partners, employees, and users of digital platforms in accordance with the legislation of Ukraine and international standards in the field of personal data protection, in particular the requirements of the GDPR, when carrying out international activities or processing data of persons from European Union countries.

1.2. Dual Regime of Legal Regulation

1.2.1. The Organization is registered in Ukraine, yet conducts activities in Ukraine, Poland, and other EU countries, offers services to natural persons in the EU, and monitors the behavior of users of digital platforms within the EU. Accordingly, pursuant to Article 3 GDPR (extraterritorial scope), the activities of the Organization fall under the direct applicability of the GDPR.

1.2.2. At the same time, as a legal entity resident in Ukraine, the Organization is obliged to comply with Law No. 2297-VI and with the subordinate legislation of the Commissioner of the Verkhovna Rada of Ukraine for Human Rights.

1.2.3. In the event of any discrepancy between the GDPR and Law No. 2297-VI, the Organization shall apply the norm that provides the higher level of protection for the rights of the data subject.

1.3. Scope of Application

1.3.1. The Regulation applies to the processing of any personal data carried out by the Organization:

- within the activities of the headquarters in Ukraine;
- within the activities of the Krakow and other separate subdivisions on the territory of the EU;
- on the digital platforms, websites (rukh.global), and mobile applications of the Organization;
- within projects funded by the EU, UN agencies, GIZ, SIDA, and other donors.

1.3.2. The Regulation is mandatory for:

- all staff employees of the Organization;
- persons performing work under civil-law contracts / service agreements;
- volunteers;
- members of the Management Board and the Head of the Organization;
- counterparties, contractors, and partners — to the extent defined by Data Processing Agreements (DPAs).

2. REGULATORY FRAMEWORK

2.1. This Regulation is developed on the basis of the following regulatory and legal acts and standards:

2.1.1. European Union Legislation

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR);

- Directive (EU) 2016/680 — Law Enforcement Directive (applicable to processing of data for law enforcement purposes; low relevance for RUKH Global);
- Directive 2002/58/EC (ePrivacy Directive) as amended by Directive 2009/136/EC — regulates cookies, electronic marketing, and electronic communications;
- European Data Protection Board (EDPB) Guidelines — advisory documents on the application of the GDPR;
- Standard Contractual Clauses (SCCs) — Commission Implementing Decision (EU) 2021/914.

2.1.2. Legislation of Ukraine

- Constitution of Ukraine (Article 32 — the right to inviolability of private life);
- Law of Ukraine "On Personal Data Protection" No. 2297-VI of 01 June 2010 (current wording);
- Law of Ukraine "On Information" No. 2657-XII of 02 October 1992;
- Law of Ukraine "On Access to Public Information" No. 2939-VI of 13 January 2011;
- Law of Ukraine "On Electronic Communications" No. 1089-IX of 16 December 2020;
- Order of the Commissioner of the Verkhovna Rada of Ukraine for Human Rights No. 1/02-14 of 08 January 2014 "On the Approval of Documents in the Field of Personal Data Protection" (Standard Procedure for Processing Personal Data; Procedure for the Commissioner's Supervision of Compliance with Personal Data Protection Legislation; Procedure for Notification of the Commissioner on Processing of Personal Data that Presents Particular Risk);
- Criminal Code of Ukraine (Article 182 — violation of the inviolability of private life);
- Code of Ukraine on Administrative Offences (Articles 188-39, 188-40 — violation of personal data protection legislation).

2.1.3. Charter of the Organization and Internal Documents

- Charter of NGO "RUKH Global" (Clause 3.2.7);
- Code of Ethics and Conduct;
- IT and Information Security Policy;
- Human Resources Policy;
- Whistleblowing Policy.

2.1.4. International Standards

- ISO/IEC 27001:2022 — Information Security Management Systems;
- ISO/IEC 27701:2019 — Privacy Information Management;
- Core Humanitarian Standard (CHS) — standard for work with beneficiaries.

3. KEY TERMS AND DEFINITIONS

3.1. The following terms are used in this Regulation (with meanings harmonized with the GDPR and Law No. 2297-VI):

Term	**Definition**
Personal data	Any information relating to an identified or identifiable natural person (name, identifier, geolocation, IP address, photograph, online identifier, etc.) — Article 4(1) GDPR; Article 2 of Law No. 2297-VI.
Special categories of data	Data revealing racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, data concerning health, sex life, or sexual orientation — Article 9 GDPR.
Processing	Any operation performed on personal data: collection, recording, organization, structuring, storage, adaptation, retrieval, use, dissemination, erasure, etc. — Article 4(2) GDPR.
Controller	A natural or legal person who alone or jointly with others determines the purposes and means of processing personal data. For the purposes of this Regulation, the Controller is NGO "RUKH Global".
Processor	A person who processes data on behalf of the Controller (cloud services, contractors, accounting firms, etc.).
Data subject	A natural person to whom the personal data relates.
Consent	A freely given, specific, informed, and unambiguous indication of the data subject's wishes, expressed by a clear affirmative action (opt-in) — Articles 4(11), 7 GDPR.
Legitimate interest	A legal basis for processing based on the balance of interests of the Controller and the data subject — Article 6(1)(f) GDPR.

DPIA (Data Protection Impact Assessment)	Assessment of the impact of processing on data protection — Article 35 GDPR.
Data breach	A breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data — Article 4(12) GDPR.
Right to erasure (Right to be forgotten)	The data subject's right to request erasure of their data — Article 17 GDPR.
DPO (Data Protection Officer)	The officer responsible for personal data protection — Articles 37–39 GDPR.
ROPA	Record of Processing Activities — register of processing operations (Article 30 GDPR).
DPA (Data Processing Agreement)	Agreement on the processing of personal data between the Controller and the Processor — Article 28 GDPR.
SCCs (Standard Contractual Clauses)	Standard contractual clauses of the European Commission for cross-border data transfers.

4. PRINCIPLES OF PERSONAL DATA PROCESSING

4.1. The Organization processes personal data in accordance with the principles set out in Article 5 GDPR and Article 6 of Law No. 2297-VI:

4.1.1. Lawfulness, Fairness, and Transparency

Processing is carried out on a lawful legal basis (Section 5 of this Regulation); data subjects are provided with full and clear information about the processing (Privacy Notice).

4.1.2. Purpose Limitation

Data are collected for specified, explicit, and legitimate purposes and are not further processed in a manner incompatible with those purposes.

4.1.3. Data Minimisation

The volume of data is limited to what is adequate, relevant, and necessary for the achievement of the purpose. The collection of excessive data is prohibited.

4.1.4. Accuracy

The Organization takes reasonable steps to ensure the accuracy and updating of data. Inaccurate data shall be corrected or erased without delay.

4.1.5. Storage Limitation

Data are kept in a form that permits identification of data subjects for no longer than is necessary for the purposes of the processing (see Section 11 — Retention Schedule, Annex I).

4.1.6. Integrity and Confidentiality

Data are protected by appropriate technical and organizational measures (TOMs, Section 15) against unauthorized access, destruction, or damage.

4.1.7. Accountability

The Controller bears responsibility for compliance with the principles and shall be able to demonstrate such compliance (documentation, registers, training, audits).

5. LEGAL BASES FOR PROCESSING

5.1. The Organization processes personal data only where at least one of the legal bases provided for in Article 6 GDPR and Article 11 of Law No. 2297-VI is in place.

Legal basis	**When it applies at RUKH Global**	**Example**
Consent — Article 6(1)(a)	Marketing, newsletters, photo/video at events, storytelling	Newsletter subscription via form on rukh.global; consent to publish photos from a festival
Contract — Article 6(1)(b)	Performance of employment contracts, civil-law contracts, volunteer agreements, grant agreements with beneficiaries	Payment of salary; payment of remuneration to contractors

Legal obligation — Article 6(1)(c)	Tax reporting, mandatory social insurance, military registration, accounting, reporting to donors	Submission of Form 1-DF; ESV (Unified Social Contribution); financial report to donor
Vital interests — Article 6(1)(d)	Humanitarian crisis situations; medical assistance to IDPs	Provision of emergency medical aid to a beneficiary
Public task — Article 6(1)(e)	Rare; individual public projects / advocacy	Public reports; advocacy campaigns
Legitimate interests — Article 6(1)(f)	Operational needs, IT security, fundraising among existing donors	Video surveillance in the office; access logging

5.2. Consent

5.2.1. Consent shall be freely given, specific, informed, unambiguous, and expressed by a clear affirmative action (opt-in).

5.2.2. Pre-ticked boxes, silence, or inactivity shall not be deemed to constitute consent.

5.2.3. The Organization maintains a register of consents received (Consent Register) — recording who, when, how, and to what provided consent.

5.2.4. The data subject is entitled to withdraw consent at any time. Withdrawal shall be as simple as the giving of consent.

5.2.5. Where the data subject is under 16 years of age (or a lower age established by national law), consent shall be given or authorized by the holder of parental responsibility.

5.3. Legitimate Interest and LIA

5.3.1. Before relying on the "legitimate interests" legal basis, the Organization conducts a Legitimate Interests Assessment (LIA), which consists of three tests:

- Purpose test — is the interest legitimate?
- Necessity test — is the processing necessary?
- Balancing test — do the interests or fundamental rights of the data subject override?

5.3.2. Results of the LIA are documented and retained by the DPO.

6. SPECIAL CATEGORIES OF DATA (ARTICLE 9 GDPR)

6.1. The processing of special categories of data is prohibited, except in the cases provided for in Article 9(2) GDPR, in particular:

- explicit consent of the data subject;
- necessity for the performance of obligations in the field of employment and social security law;
- protection of the vital interests of the data subject where the data subject is incapable of giving consent;
- processing within the lawful activities of non-profit organizations with a political, philosophical, religious, or trade-union aim — only in respect of members, former members, or persons with regular contact with the organization;
- data manifestly made public by the data subject;
- establishment, exercise, or defense of legal claims;
- substantial public interest.

6.2. Particularly sensitive categories for RUKH Global:

- data concerning health (beneficiaries of art therapy programs, veteran rehabilitation);
- data on ethnic origin (Ukrainian diaspora, internally displaced persons — IDPs);
- political opinions (participants of advocacy campaigns);
- data concerning children (in Creative Europe and Erasmus+ projects with children's participation).

6.3. When processing data of IDPs, children, and other vulnerable groups, additional safeguards apply (safeguarding, concealment of surnames in reports, use of pseudonym-IDs).

7. CATEGORIES OF DATA SUBJECTS

7.1. The Organization processes personal data of the following categories of data subjects:

Category	**Examples**
Staff employees	Senior management, project managers, communications team, finance team

Persons under civil-law / service contracts	Trainers, coaches, designers, translators, IT contractors
Volunteers	Participants of volunteer programs in Ukraine and abroad
Program beneficiaries	IDPs, veterans, participants of rehabilitation programs, diaspora youth
Partners	Representatives of partner NGOs, state bodies, international organizations
Donors (natural persons)	Individuals making donations
Event participants	Participants of conferences, festivals, seminars
Newsletter subscribers	Persons subscribed to the rukh.global newsletter
Candidates for vacancies	CVs, motivation letters
Users of digital platforms	Registered users of the mobile application and website
Members of the Organization	Full and associate members in accordance with the Charter (Clause 4.2)

8. CATEGORIES OF PERSONAL DATA

8.1. The Organization processes the following categories of data (the scope depends on the category of the data subject and the legal basis):

Category of data	**Examples**
Identification	Name, date of birth, Taxpayer Registration Number (RNOKPP / TIN), passport data, driver's license number
Contact	Address, telephone, email, messengers, social networks
Professional / HR	Position, CV, education, experience, employment record book, military registration
Financial	Bank account, IBAN, tax information, payment history
Online / technical	IP address, cookies, browser, device, geolocation, logs
Media	Photos, videos, audio recordings from events
Special categories	Health data (for beneficiaries), political opinions, ethnic origin
Contractual / project-related	Beneficiary status, participation in a project, participation outcomes

9. SOURCES OF DATA COLLECTION

9.1. The Organization obtains personal data from the following sources:

- directly from the data subject (applications, registration forms, questionnaires, contracts, email correspondence);
- public registers and open sources (register of legal entities, official websites);
- from partner organizations — exclusively on the basis of concluded data-sharing agreements / DPAs, where the partner has a valid legal basis;
- from public authorities (embassies, consulates — in the case of data processing for IDPs and refugees);
- automatically (cookies, analytics, server logs — with notification and consent where required).

9.2. Where data are obtained other than from the data subject, the Organization shall provide the data subject with a Privacy Notice indicating the source within a reasonable period, but no later than 30 days (Article 14 GDPR).

10. TRANSFER OF DATA TO THIRD PARTIES

10.1. Transfer to Processors

10.1.1. The Organization engages processors (cloud services, accounting and legal contractors, email platforms, CRM) solely on the basis of a concluded Data Processing Agreement (DPA) — see Annex C.

10.1.2. The DPA is concluded in accordance with Article 28 GDPR and contains the mandatory elements: subject matter, duration, nature, purpose of processing, type of data, categories of data subjects, and the obligations and rights of the Controller.

10.1.3. The engagement by a processor of sub-processors is permitted only with the prior written consent of the Controller.

10.2. Transfer to Partners

10.2.1. The transfer of data to partners within joint projects is carried out on the basis of:

- Grant Agreement / Consortium Agreement with the donor (which authorizes the exchange of data between partners);

- a separate DPA or Data Sharing Agreement;
- in a joint controllers model (Article 26 GDPR) — additionally, a Joint Controllership Agreement.

10.3. Transfer to Donors and Public Authorities

10.3.1. Reporting to donors (EU, UN agencies, GIZ, SIDA) is carried out on the basis of the Grant Agreement. By default, the Organization transfers aggregated / anonymized data; personal data are transferred only where this is expressly provided for by the Grant Agreement.

10.3.2. Transfers to public authorities are carried out exclusively on the basis of a written request with reference to a statutory provision.

10.4. Cross-Border Transfer

10.4.1. Transfers within the European Economic Area (EEA) are carried out freely.

10.4.2. Transfer from Ukraine to the EU. As of 2026, the European Commission has not adopted a general adequacy decision in respect of Ukraine; transfers are carried out on the basis of Article 49 GDPR (derogations) or SCCs.

10.4.3. Transfers outside the EEA (United States, United Kingdom, others) are carried out on one of the following bases:

- an adequacy decision of the European Commission (e.g., UK adequacy decision, EU-US Data Privacy Framework);
- Standard Contractual Clauses (SCCs) 2021/914;
- Binding Corporate Rules (BCRs);
- derogations under Article 49 (explicit consent, necessity for performance of a contract, etc.).

10.4.4. Prior to any cross-border transfer, a Transfer Impact Assessment (TIA) shall be conducted.

11. RETENTION PERIODS

11.1. Retention periods for personal data are determined in accordance with the purposes of processing, statutory requirements, and donor requirements. The general table is provided in Annex I.

Category	Retention period	Basis
Employee personnel files	75 years	Standard Documents List of the Ministry of Justice, 2021
Primary HR documents (time sheets, schedules)	5 years	Legislation of Ukraine
Primary accounting documents	3 years (general) / 5 years (Clause 44.3 of the Tax Code)	Tax Code of Ukraine; Law No. 996-XIV
Bank statements, agreements with donors	7–10 years	Grant agreements
Marketing newsletter subscriber data	Until consent withdrawal + 1 year (archive)	Consent withdrawal
Job applications (unsuccessful)	6 months (with explicit consent — up to 1 year)	EU practice
Project data (EU grants)	10 years after project closure	EU Financial Regulation 2024/2509
Cookies (session)	Until browser closure	ePrivacy
Cookies (analytics)	13–26 months	Cookie Policy
IT system logs	12 months	IT security
Office video surveillance	30 days	Legitimate interest
Data Breach Register	5 years	Accountability
Consent Register	Data retention period + 3 years	Accountability
DSAR Register	3 years after request fulfilment	Accountability

11.2. Erasure and Anonymization

11.2.1. Upon expiry of the retention period, data shall be irreversibly erased or anonymized (pseudonymization / anonymization).

11.2.2. The destruction of physical media is formalized by an Act of Destruction signed by the DPO and the responsible employee.

11.2.3. For digital media, cryptoshredding (destruction of encryption keys) or secure wipe in accordance with NIST SP 800-88 is applied.

11.2.4. Erasure of data in cloud services is initiated by means of deletion and is confirmed by the processor.

12. RIGHTS OF DATA SUBJECTS

12.1. Data subjects enjoy the following rights under Articles 15–22 GDPR and Article 8 of Law No. 2297-VI:

Right	Description
Right to information (Articles 13–14)	To receive a Privacy Notice at the point of data collection
Right of access (Article 15)	To obtain a copy of data and information about processing
Right to rectification (Article 16)	To request the correction of inaccurate data
Right to erasure / to be forgotten (Article 17)	To request erasure where there is no ground for further processing
Right to restriction of processing (Article 18)	To request temporary restriction of processing
Right to data portability (Article 20)	To receive data in a structured format (JSON, CSV) and transmit to another controller
Right to object (Article 21)	To object to processing based on legitimate interests or to direct marketing
Right not to be subject to automated decision-making (Article 22)	Including profiling with legal effects
Right to lodge a complaint	With the Commissioner of the Verkhovna Rada of Ukraine for Human Rights or with an EU supervisory authority (DPA) in the country of residence

12.2. Procedure for Submitting and Handling Requests (DSAR)

12.2.1. The data subject may submit a request via:

- email: privacy@rukh.global (primary channel);
- an online form at rukh.global/privacy;
- a paper letter to the legal address of the Organization.

12.2.2. Request form — Annex E. A free-form request is also accepted.

12.2.3. The DPO verifies the identity of the requestor (via a copy of identification, email confirmation, or security questions).

12.2.4. A response shall be provided within 30 calendar days of receipt of the request. In complex cases, the period may be extended by a further 60 days with a written justification.

12.2.5. The response is provided in the same format as the request, or in the format requested.

12.2.6. Services are provided free of charge. A fee may be charged only for manifestly unfounded or repetitive requests.

12.2.7. In the event of refusal, the DPO shall substantiate the decision and inform of the right to appeal to the supervisory authority and to court.

12.2.8. All requests are recorded in the DSAR Register (Data Subject Access Requests Register).

13. DPIA — DATA PROTECTION IMPACT ASSESSMENT

13.1. A DPIA (Data Protection Impact Assessment) shall be carried out OBLIGATORILY prior to the commencement of processing where the processing is likely to result in a high risk to the rights and freedoms of data subjects (Article 35 GDPR). In particular:

- systematic and extensive monitoring of behavior (web tracking, CCTV, location tracking);
- large-scale processing of special categories of data (health, political opinions);
- systematic processing of data in publicly accessible areas;
- implementation of new technologies (AI, big data, biometrics);
- processing of data of vulnerable groups (children, IDPs, persons with disabilities);
- profiling resulting in legal consequences.

13.2. Examples where a DPIA is required for RUKH Global:

- launch of a new mobile application with geolocation tracking of diaspora members;

- analysis of user behavior on a platform with AI-based recommendations;
- processing of medical data of veterans in art therapy programs;
- CCTV video surveillance at event venues.

13.3. Structure of the DPIA (Annex D):

- systematic description of the processing operation and purposes;
- assessment of necessity and proportionality;
- identification of risks to rights and freedoms;
- risk mitigation measures.

13.4. Where, following the DPIA, the residual risk remains high, the Organization shall conduct a prior consultation with the Commissioner of the Verkhovna Rada of Ukraine for Human Rights (in Ukraine) or an EU supervisory authority (Article 36).

14. PRIVACY BY DESIGN AND BY DEFAULT

14.1. The Organization implements the principles of Privacy by Design and Privacy by Default (Article 25 GDPR) at all stages of the development of products, processes, and partnerships.

14.2. Privacy by Design:

- personal data protection is taken into account at the stage of designing the IT system or process;
- data minimization, pseudonymization, and encryption are implemented at the technological level.

14.3. Privacy by Default:

- by default, only data necessary for the specific purpose are processed;
- all privacy settings on RUKH Global digital platforms are set by default to the highest level of protection;
- data are not made publicly available without an active action by the data subject.

15. TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

15.1. The Organization implements a set of technical and organizational measures (Article 32 GDPR) to ensure the security of processing, commensurate with the risks. The TOMs checklist is provided in Annex G.

15.2. Technical Measures

- encryption of data at rest (disks, databases) and in transit (HTTPS/TLS 1.3);
- multi-factor authentication (MFA) for all accounts with access to personal data;
- centralized access management (Identity & Access Management), role-based access control (RBAC);
- backup and disaster recovery — at least once every 24 hours, with a test restoration once per quarter;
- logging of access, modification, and erasure of data;
- antivirus protection, EDR, automated updates of OS and software;
- network segmentation; VPN for remote access;
- pseudonymization / anonymization in reports, dashboards, and research;
- data loss prevention (DLP) for sensitive channels.

15.3. Organizational Measures

- appointed DPO (Section 17);
- clean desk and clean screen policy;
- NDAs for all employees, contractors, and volunteers;
- training (onboarding + annual refresh);
- onboarding/offboarding procedure for personnel with access management;
- periodic audit (annually) and penetration testing (once every 2 years).

16. COOKIES AND ELECTRONIC MARKETING

16.1. The rukh.global website applies a cookie consent banner that complies with the requirements of the ePrivacy Directive and the GDPR.

16.2. Cookies are classified into the following categories:

- strictly necessary — no consent required;
- performance / analytics — subject to prior consent (opt-in);
- marketing / advertising — subject to prior consent;
- functional — subject to prior consent.

16.3. Full information is provided in the Cookie Policy (Annex H), available at rukh.global/cookies.

16.4. Email marketing (newsletters) is carried out only on the basis of an explicit opt-in consent. Every message contains an unsubscribe button.

17. DATA PROTECTION OFFICER (DPO)

17.1. The Organization appoints a Data Protection Officer (DPO) in accordance with Articles 37–39 GDPR. For RUKH Global, the appointment of a DPO is recommended (in view of the scale of processing, including special categories of data of beneficiaries and monitoring of behavior through digital platforms).

17.2. Qualification Requirements for the DPO

- expert knowledge of personal data protection legislation (GDPR, Law No. 2297-VI);
- minimum 3 years of experience in compliance / data protection;
- certification (CIPP/E, CIPM, ISO 27701 Lead Implementer — desirable);
- proficiency in Ukrainian and English languages.

17.3. Forms of Appointment

- internal DPO — a staff employee without conflict of interests (may not be the head of IT, HR, or Finance);
- external DPO — under a civil-law contract with a legal or natural person.

17.4. Functions of the DPO

- informing and advising the Controller and employees of their obligations;
- monitoring compliance;
- advising on DPIAs;
- cooperation with the Commissioner of the Verkhovna Rada of Ukraine and EU supervisory authorities;
- acting as the contact point for data subjects;
- maintaining the ROPA, DSAR Register, Breach Register, and Consent Register.

17.5. DPO contact: privacy@rukh.global.

17.6. The DPO reports directly to the Executive Director and the Chairman of the Management Board.

18. PERSONAL DATA BREACH NOTIFICATION

18.1. A data breach (personal data security breach) is a breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

18.2. Response Procedure (full Response Plan — Annex F)

18.2.1. Step 1 (T+0 h): detection → immediate notification of the DPO and the IT administrator.

18.2.2. Step 2 (T+0–24 h): containment — isolation of affected systems, stopping the leak.

18.2.3. Step 3 (T+0–48 h): assessment — scale, data categories, number of data subjects, likely consequences.

18.2.4. Step 4 (T+0–72 h): notification:

- notification to the Commissioner of the Verkhovna Rada of Ukraine for Human Rights (in Ukraine) and/or the EU supervisory authority (lead supervisory authority) WITHIN 72 HOURS of detection;
- where the breach entails a high risk to the rights of data subjects — immediate notification of the data subjects themselves (Article 34 GDPR);
- where notification within 72 hours is not feasible — a written justification for the delay.

18.2.5. Step 5: remediation — elimination of causes, restoration.

18.2.6. Step 6: post-incident review — analysis, conclusions, updating of TOMs.

18.3. Content of Notification to the Regulator

- nature of the breach, categories and approximate number of data subjects and records concerned;
- DPO contact;
- likely consequences;
- measures taken / proposed.

18.4. Breach Register

The DPO maintains a Breach Register of all incidents (including those not requiring notification), with a retention period of 5 years.

19. CONTRACTORS AND POST-EMPLOYMENT OBLIGATIONS

19.1. All employees, persons under civil-law contracts, volunteers, and contractors sign a Non-Disclosure Agreement (NDA) that includes provisions on the confidentiality of personal data.

19.2. Obligations to maintain confidentiality shall continue INDEFINITELY after the termination of the employment or contractual relationship.

19.3. Upon termination of the relationship, the employee shall return all media containing personal data and delete data from personal devices (BYOD).

19.4. An offboarding procedure is performed: revocation of all access rights within 24 hours, rotation of keys / passwords.

20. STAFF TRAINING

20.1. The Organization ensures mandatory personal data protection training for all persons with access to data.

20.2. Training format:

- induction — within the first 14 days after employment or the commencement of volunteering;
- annual refresh — once per calendar year;
- targeted training following critical incidents or changes in legislation.

20.3. Content of the training:

- principles of the GDPR and Law No. 2297-VI;
- rules for the collection, processing, storage, and transfer of data;
- rights of data subjects and the procedure for handling DSARs;
- data breach response procedure;
- technical rules (passwords, MFA, phishing awareness).

20.4. Following the training, the employee takes a test and signs an acknowledgement. Records are maintained by HR / DPO.

21. REGISTERS

21.1. The Organization maintains the following mandatory registers:

Register	**Description**
ROPA (Article 30 GDPR)	Register of all processing activities (who, what data, for what purpose, basis, retention, transfer). Template — Annex F.
Consent Register	Register of consents received: who, when, to what, channel, wording version
DSAR Register	Register of requests from data subjects
Breach Register	Register of security incidents
LIA Register	Register of Legitimate Interests Assessments conducted
DPIA Register	Register of Data Protection Impact Assessments conducted
TIA Register	Register of Transfer Impact Assessments
Training Log	Records of training completion
Vendor / DPA Register	Records of processors and DPAs concluded

21.2. All registers are maintained by the DPO in electronic form with version control.

21.3. Registers shall be provided to the Commissioner of the Verkhovna Rada of Ukraine / the EU supervisory authority upon request.

22. RESPONSIBILITY

22.1. The Controller (NGO "RUKH Global") bears overall responsibility for compliance with this Regulation and with personal data protection legislation.

22.2. The Chairman of the Management Board:

- approves the Regulation and material amendments thereto;
- ensures resources for the implementation of the Regulation.

22.3. The Executive Director:

- ensures operational implementation;
- appoints the DPO;
- approves related procedures.

22.4. The DPO:

- coordinates implementation;
- maintains registers, conducts DPIAs, trains staff;
- serves as the contact point for data subjects and regulators.

22.5. Each employee, volunteer, and contractor is responsible for compliance with the Regulation within the scope of their duties.

22.6. Violations of personal data protection legislation may entail:

- disciplinary, civil, administrative (Articles 188-39, 188-40 of the Code of Ukraine on Administrative Offences), and criminal (Article 182 of the Criminal Code of Ukraine) liability under Ukrainian law;
- administrative fines under the GDPR — up to EUR 20 million or 4% of annual worldwide turnover (whichever is higher);
- civil claims by data subjects for compensation of damages.

23. FINAL PROVISIONS

23.1. This Regulation enters into force upon approval by the Management Board of NGO "RUKH Global" and signature by the Chairman of the Management Board.

23.2. The Regulation shall be reviewed at least once every 2 years or upon:

- material changes in the legislation of Ukraine or EU law;
- material changes in the activities of the Organization;
- significant incidents (data breach);
- recommendations from donor audits.

23.3. Amendments to the Regulation are approved by the Management Board.

23.4. Upon entry into force, all previous internal documents that contradict this Regulation shall cease to have effect in the relevant part.

23.5. The signed original of the Regulation shall be kept by the DPO / legal department. The current version shall be published on the internal portal and shall be made available to staff upon request.

23.6. Person responsible for the Regulation: DPO of NGO "RUKH Global" — privacy@rukh.global.

ANNEX A. PRIVACY NOTICE (TEMPLATE)

For: employees / volunteers / beneficiaries / event participants (to be adapted as required)

1. Who we are

Controller of personal data: Non-governmental organization "RUKH Global", registered address: Ukraine, 08290, Kyiv Region, Bucha District, Hostomel, 12A Patriotiv St. Contact: hello@rukh.global. DPO: privacy@rukh.global.

2. What data we process

[Specify the particular categories: full name, email, telephone, photograph, IBAN, etc.]

3. For what purpose

[For example: performance of the employment contract; sending of the newsletter; implementation of grant project XYZ funded by Creative Europe]

4. Legal basis

[Article 6(1)(b) — contract / Article 6(1)(a) — consent / Article 6(1)(c) — legal obligation / Article 6(1)(f) — legitimate interest]

5. To whom we transfer data

[Specific categories of recipients: bank, tax authority, donor, cloud provider Google Workspace (EU/US under the EU-US Data Privacy Framework)]

6. How long we retain data

[Retention period — with reference to the Retention Schedule]

7. Cross-border transfer

[Countries outside the EEA; basis: SCCs / adequacy decision]

8. Your rights

You have the rights of access, rectification, erasure, restriction of processing, portability, objection, withdrawal of consent, and lodging a complaint with the Commissioner of the Verkhovna Rada of Ukraine for Human Rights or an EU supervisory authority in the country of residence.

9. How to contact us

Email: privacy@rukh.global. Response — within 30 days.

ANNEX B. CONSENT FORM

I, _____ (full name), provide my freely given, specific, informed, and unambiguous consent to NGO "RUKH Global" (Controller) for the processing of my personal data for the following purposes (tick as appropriate):

☐ 1. Receiving the RUKH Global email newsletter

☐ 2. Publication of my photographs / video taken at Organization events on social networks, the website, and in donor reports

☐ 3. Transfer of my data to partners of the Organization within a specific project: _____

☐ 4. Processing of special categories of data (health) within the framework of the program _____ (if applicable)

☐ 5. Transfer of my data outside the EEA (to the United States / other countries) on the basis of SCCs

I have been informed of the right to withdraw consent at any time by sending a message to privacy@rukh.global without adverse consequences, as well as of all other rights of the data subject under Articles 15–22 GDPR.

Date: _____ Signature: _____ Name in print: _____

Internal section: Received by: _____ Channel of receipt: □ online form □ email □ paper Wording version: v1.0

ANNEX C. DATA PROCESSING AGREEMENT (DPA) — BRIEF TEMPLATE

Concluded between NGO "RUKH Global" (Controller) and _____ (Processor) in accordance with Article 28 GDPR.

1. Subject matter and duration

The Processor processes personal data on behalf of the Controller in the course of providing services under the main Agreement No. ___ of ___.

2. Nature and purpose of processing

[Specify, for example: data hosting, payment processing, email campaigns]

3. Types of data and categories of data subjects

[Name, email, telephone; employees, beneficiaries, etc.]

4. Obligations of the Processor (Article 28(3) GDPR)

- to process data only on documented instructions of the Controller;
- to ensure the confidentiality of persons with access to the data;
- to take all necessary security measures (Article 32);
- to engage sub-processors only with prior written consent;

- to assist the Controller in fulfilling data subjects' requests;
- to assist with DPIAs and prior consultations;
- to notify of a data breach within 24 hours of detection;
- upon termination of services — to delete or return the data at the Controller's choice;
- to provide access to information and to permit audits.

5. Sub-processors

List of pre-approved sub-processors: _____

6. Cross-border transfer

Transfer outside the EEA — on the basis of SCCs 2021/914, Module ___.

7. Term and termination

The DPA remains in effect for the duration of the main Agreement. Confidentiality obligations are indefinite.

Date: _____ For the Controller: _____ For the Processor: _____

ANNEX D. DPIA TEMPLATE (ABRIDGED)

Section	Description
1. Name of the process / project	
2. Description of processing	Data flows, systems, categories of data subjects, data, purposes
3. Legal basis	
4. Necessity and proportionality	Can the purpose be achieved with less data / less risky means?
5. Stakeholder consultation	Have data subjects / DPO / partners been consulted?
6. Risk analysis	Identification of threats, likelihood, consequences for data subjects' rights
7. Risk mitigation measures	TOMs, pseudonymization, training, contracts
8. Residual risk	Low / Medium / High
9. Need for prior consultation	Yes / No
10. Signatures	DPO: _____ Date: _____ Process owner: _____

ANNEX E. DSAR FORM (DATA SUBJECT ACCESS REQUEST)

To NGO "RUKH Global", DPO — privacy@rukh.global

I, _____ (full name), identifier (email/telephone): _____, request the following (tick as appropriate):

- provide access to my personal data (Article 15 GDPR);
- rectify inaccurate data (Article 16): _____;
- erase my personal data (Article 17);
- restrict processing (Article 18);
- provide my data in a structured format (Article 20);
- cease processing on the basis of my rights (Article 21);
- other: _____.

Basis / details: _____

Preferred response channel: □ email □ paper mail

I attach an identity document (copy of passport — for verification): □ yes

Date: _____ Signature: _____

Internal section (DPO):

Received: _____ Request ID: _____ Verification: □ successful □ unsuccessful Response date: _____ Outcome: _____

ANNEX F. ROPA — REGISTER TEMPLATE (ARTICLE 30 GDPR)

Process	Purpose	Legal basis	Categories of subjects and data	Retention	Recipients / transfer
HR — employment relations	Performance of contract, taxes	Art. 6(1)(b), (c)	Employees: name, passport, TIN, IBAN	75 y. / 5 y.	Bank, State Tax Service, Pension Fund
Volunteer management	Coordination of volunteers	Art. 6(1)(b)	Volunteers: name, email, telephone	Period + 3 y.	Project partners (DPA)
Email newsletter	Marketing	Art. 6(1)(a)	Subscribers: email, name	Until opt-out + 1 y.	Mailchimp / Brevo
Beneficiary register	Implementation of programme	Art. 6(1)(b), 9(2)(g)	Beneficiaries: name, IDP status, health	10 y. after project closure	Donor (reports)
Website analytics	Website improvement	Art. 6(1)(a) / (f)	Visitors: IP, cookies	26 months	Google (EU-US DPF)

ANNEX G. DATA BREACH RESPONSE PLAN (STEP-BY-STEP)

Step	Time (T = detection)	Action	Responsible
1	T + 0 h	Detection and immediate notification of DPO and IT	Any employee → DPO, IT
2	T + 0–2 h	Containment: isolation of systems, blocking of accounts, key rotation	IT + DPO
3	T + 2–24 h	Assessment: what happened, which data, how many subjects, what risk	DPO + IT
4	T + 24–48 h	Risk classification: low / medium / high	DPO
5	T + 48–72 h	Notification — Commissioner of the Verkhovna Rada / EU supervisory authority	DPO
6	T + 0–7 days	Notification of data subjects where risk is high (Article 34)	DPO + Communications
7	T + 1–30 days	Remediation, updating of TOMs, communication with partners	IT + Management
8	T + 30–45 days	Post-incident review, updating of Breach Register	DPO

Criteria of "high risk" for the subject: possibility of financial harm, identity theft, reputational damage, disclosure of special categories of data.

ANNEX H. TOMs CHECKLIST

#	Measure	Status	Review date
1	Full-disk encryption — BitLocker / FileVault		
2	TLS 1.3 for all communications		
3	MFA for all accounts with access to PII		
4	Enterprise password manager		
5	RBAC — roles and rights documented		
6	Regular backups + restoration tests (quarterly)		
7	Centralized logging and monitoring		
8	Antivirus / EDR on all devices		
9	Auto-updates of OS and software		
10	VPN for remote access		
11	NDA in all employment / civil-law contracts		
12	Onboarding / offboarding checklist for access rights		
13	GDPR training — induction + annual refresh		
14	Clean desk / clean screen policy		

15	Phishing simulations (at least twice a year)		
16	Penetration testing (once every 2 years)		
17	Inventory of systems / data (once a year)		
18	BYOD policy and MDM		
19	DLP for sensitive channels		
20	Cookie consent banner on rukh.global		

ANNEX I. COOKIE POLICY (BRIEF TEMPLATE FOR RUKH.GLOBAL)

1. We use cookies and similar technologies on the rukh.global website to ensure functionality, analytics, and marketing.

2. Categories of cookies:

Category	Purpose	Consent	Duration
Strictly necessary	Session authentication, security	Not required	Session
Performance / Analytics	Google Analytics 4 — visit statistics	Opt-in	13 months
Marketing	Meta Pixel, Google Ads — retargeting	Opt-in	26 months
Functional	Language / theme preferences	Opt-in	12 months

3. You may modify or withdraw consent at any time via the cookie banner or Privacy Settings.

4. Contact: privacy@rukh.global.

ANNEX J. RETENTION SCHEDULE (EXTENDED TABLE)

Data category	Retention period	Basis	Note
Employment contracts, orders	75 years	Standard Documents List	For pension record
Personnel file	75 years	Legislation	
Time sheets, schedules, leave records	5 years	Labour Code; Law No. 996-XIV	
Civil-law contracts	3 years (with payment documents — 5)	Civil Code + Tax Code	
Job applications	6 months / 12 months with consent	GDPR practice	
Reference letters	6 months	Minimization	
Primary accounting documents	5 years	Tax Code, Clause 44.3	
Bank statements	5 years	Tax Code	
Reports to EU donors	10 years after project closure	EU FR 2024/2509	
Grant agreements — USAID / State Dept.	10 years	2 CFR 200	
Marketing subscribers	Until opt-out + 1 year	Consent	Archive with minimized data
Event participants (without consent for further contact)	1 year after the event	Donor reports	
Event photos / videos	5 years (with consent) / until withdrawal	Consent	
Video surveillance	30 days	Legitimate interest	Cyclical overwrite
IT logs	12 months	Security	
Cookies (analytics)	13–26 months	Consent	Depends on tool
Cookies (strictly necessary)	Session	Art. 6(1)(f)	
Breach Register	5 years	Accountability	
Consent Register	PII retention period + 3 years	Accountability	
DSAR Register	3 years after request closure	Accountability	
DPIA documents	Processing period + 3 years	Accountability	

NDAs	10 years after termination	Civil law	
Statutory documents	Permanently	Law No. 4572-VI	

All employees have been familiarized with the Regulation (acknowledgement sheet maintained by HR).

Person responsible for the Regulation: DPO — privacy@rukh.global
Next scheduled review: April 2028