NGO «RUKH Global»

hello@rukh.global
www.rukh.global

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

ЗАТВЕРДЖЕНО

Рішенням Правління
ГО «РУКХ Глобал»
Протокол № 3 від 17» квітня 2026 р.

Голова Правління
_____ І. Дудка

Виконавчий Директор
_____ М. Махота

ПОЛОЖЕННЯ

ПРО ОБРОБКУ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «РУКХ ГЛОБАЛ»

GDPR (Regulation (EU) 2016/679) + ЗУ № 2297-VI

Версія 1.0

Дата набрання чинності: «___» _____ 2026 р.

Київ — 2026

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Призначення та мета Положення

1.1.1. Це Положення про обробку та захист персональних даних (далі — Положення) визначає принципи, правила, процедури та заходи, яких дотримується Громадська організація «РУКХ Глобал» (далі — Організація, РУКХ Глобал, Контролер) при обробці персональних даних фізичних осіб (далі — суб'єкти даних).

1.1.2. Метою Положення є забезпечення дотримання вимог:

- Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних (General Data Protection Regulation, далі — GDPR);
- Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI (далі — ЗУ № 2297-VI);
- інших нормативно-правових актів України та ЄС у сфері захисту персональних даних;
- вимог донорів Організації (ЄС, ООН-агенції, GIZ, SIDA) щодо захисту персональних даних бенефіціарів, партнерів та співробітників.

1.1.3. Положення прийнято на виконання п. 3.2.7 Статуту ГО «РУКХ Глобал», яким передбачено, що Організація здійснює обробку та захист персональних даних членів, партнерів, працівників та користувачів цифрових платформ відповідно до законодавства України та міжнародних стандартів у сфері захисту персональних даних, зокрема вимог GDPR, у разі здійснення міжнародної діяльності або обробки даних осіб з країн Європейського Союзу.

1.2. Подвійний режим правового регулювання

1.2.1. Організація зареєстрована в Україні, проте здійснює діяльність в Україні, Польщі та інших країнах ЄС, пропонує послуги фізичним особам у ЄС та моніторить поведінку користувачів цифрових платформ на території ЄС. Як наслідок, згідно зі ст. 3 GDPR (extraterritorial scope / екстериторіальна дія), діяльність Організації підпадає під пряму дію GDPR.

1.2.2. Одночасно, як юридична особа-резидент України, Організація зобов'язана дотримуватися ЗУ № 2297-VI та підзаконних актів Уповноваженого Верховної Ради України з прав людини.

1.2.3. У разі розбіжностей між GDPR та ЗУ № 2297-VI Організація застосовує норму, яка забезпечує вищий рівень захисту прав суб'єкта даних.

1.3. Сфера застосування

1.3.1. Положення поширюється на обробку будь-яких персональних даних, що здійснюється Організацією:

- у межах діяльності штаб-квартири в Україні;
- у межах діяльності Краківського та інших відокремлених підрозділів на території ЄС;
- на цифрових платформах, вебсайтах (rukh.global) та у мобільних застосунках Організації;
- у рамках проєктів, що фінансуються ЄС, ООН-агенціями, GIZ, SIDA та іншими донорами.

1.3.2. Положення обов'язкове для:

- усіх штатних працівників Організації;
- осіб, які виконують роботи за договорами ЦПД / підряду;
- волонтерів;
- членів Правління та Голови Організації;
- контрагентів, підрядників, партнерів у частині, визначеній Договорами про обробку персональних даних (Data Processing Agreement, DPA).

2. НОРМАТИВНА БАЗА

2.1. Положення розроблено на підставі таких нормативно-правових актів та стандартів:

2.1.1. Законодавство Європейського Союзу

- 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 (застосовується у разі обробки даних для правоохоронних цілей, для РУКХ Глобал — низька релевантність);
- Directive 2002/58/EC (ePrivacy Directive) зі змінами Directive 2009/136/EC — регулює cookies, electronic marketing, електронні комунікації;
- European Data Protection Board (EDPB) Guidelines — рекомендаційні документи щодо застосування GDPR;
- Standard Contractual Clauses (SCCs) — Commission Implementing Decision (EU) 2021/914.

2.1.2. Законодавство України

- Конституція України (ст. 32 — право на недоторканність особистого життя);
- Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (чинна редакція);
- Закон України «Про інформацію» від 02.10.1992 № 2657-XII;
- Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI;
- Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX;
- Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» (Типовий порядок обробки персональних даних; Порядок здійснення Уповноваженим ВРУ контролю за додержанням законодавства про захист персональних даних; Порядок повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик);
- Кримінальний кодекс України (ст. 182 — порушення недоторканності приватного життя);
- Кодекс України про адміністративні правопорушення (ст. 188-39, 188-40 — порушення законодавства про захист персональних даних).

2.1.3. Статут Організації та внутрішні документи

- Статут ГО «РУКХ Глобал» (п. 3.2.7);
- Кодекс етики та поведінки;
- Політика IT та інформаційної безпеки;
- Кадрова політика;
- Whistleblowing Policy.

2.1.4. Міжнародні стандарти

- ISO/IEC 27001:2022 — Information Security Management Systems;
- ISO/IEC 27701:2019 — Privacy Information Management;
- Core Humanitarian Standard (CHS) — стандарт роботи з бенефіціарами.

3. КЛЮЧОВІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

3.1. У Положенні вживаються такі терміни (значення гармонізовано із GDPR та ЗУ № 2297-VI):

Термін	Визначення
Персональні дані (Personal data)	Будь-яка інформація, що стосується ідентифікованої або ідентифіковуваної фізичної особи (ПІБ, ідентифікатор, геолокація, IP-адреса, фото, онлайн-ідентифікатор тощо) — Art. 4(1) GDPR; ст. 2 ЗУ 2297-VI.

Термін	Визначення
Особливі категорії даних (Special categories)	Дані про расове/етнічне походження, політичні погляди, релігійні переконання, членство у профспілках, генетичні, біометричні, дані про здоров'я, статеве життя або сексуальну орієнтацію — Art. 9 GDPR.
Обробка (Processing)	Будь-яка операція з персональними даними: збір, фіксація, організація, структурування, зберігання, адаптація, пошук, використання, поширення, знищення тощо — Art. 4(2) GDPR.
Контролер (Controller)	Фізична або юридична особа, яка самостійно або разом з іншими визначає цілі та засоби обробки персональних даних. Для цього Положення Контролер = ГО «РУКХ Глобал».
Процесор (Processor)	Особа, яка обробляє дані від імені Контролера (хмарні сервіси, підрядники, бухгалтерські компанії тощо).
Суб'єкт даних (Data subject)	Фізична особа, якої стосуються персональні дані.
Згода (Consent)	Вільне, конкретне, інформоване та однозначне волевиявлення суб'єкта даних, виражене дією (opt-in) — Art. 4(11), 7 GDPR.
Легітимний інтерес (Legitimate interest)	Правова підстава обробки на підставі балансу інтересів Контролера та суб'єкта — Art. 6(1)(f) GDPR.
DPIA (Data Protection Impact Assessment)	Оцінка впливу обробки на захист даних — Art. 35 GDPR.
Data breach (Порушення безпеки)	Порушення, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних — Art. 4(12) GDPR.
Право на забуття (Right to erasure)	Право суб'єкта вимагати видалення своїх даних — Art. 17 GDPR.
DPO (Data Protection Officer)	Уповноважена особа з захисту персональних даних — Art. 37-39 GDPR.
ROPA	Record of Processing Activities — реєстр процесів обробки (Art. 30 GDPR).
DPA (Data Processing Agreement)	Договір про обробку персональних даних між Контролером та Процесором — Art. 28 GDPR.
SCCs (Standard Contractual Clauses)	Стандартні договірні положення ЄК для транскордонної передачі даних.

4. ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

4.1. Організація обробляє персональні дані згідно з принципами, визначеними ст. 5 GDPR та ст. 6 ЗУ № 2297-VI:

4.1.1. Законність, справедливість і прозорість (Lawfulness, Fairness, Transparency)

Обробка здійснюється на законній правовій підставі (п. 5 цього Положення), суб'єктам надається повна та зрозуміла інформація про обробку (Privacy Notice).

4.1.2. Обмеження метою (Purpose Limitation)

Дані збираються для конкретних, чітко визначених, законних цілей і не обробляються у спосіб, несумісний з цими цілями.

4.1.3. Мінімізація даних (Data Minimisation)

Обсяг даних обмежується тим, що є адекватним, релевантним та необхідним для досягнення мети. Збір надлишкових даних заборонений.

4.1.4. Точність (Accuracy)

Організація вживає розумних заходів для забезпечення точності даних та їх оновлення. Неточні дані невідкладно виправляються або видаляються.

4.1.5. Обмеження зберігання (Storage Limitation)

Дані зберігаються у формі, що дозволяє ідентифікацію суб'єктів, не довше, ніж це необхідно для цілей обробки (див. п. 11 — Retention Schedule, Додаток И).

4.1.6. Цілісність та конфіденційність (Integrity & Confidentiality)

Дані захищаються за допомогою належних технічних та організаційних заходів (TOMs, п. 16) від несанкціонованого доступу, знищення чи пошкодження.

4.1.7. Підзвітність (Accountability)

Контролер несе відповідальність за дотримання принципів та може це продемонструвати (документація, реєстри, навчання, аудити).

5. ПРАВОВІ ПІДСТАВИ ОБРОБКИ

5.1. Організація обробляє персональні дані лише за наявності принаймні однієї з правових підстав, передбачених Art. 6 GDPR та ст. 11 ЗУ № 2297-VI.

Правова підстава	Коли застосовується в РУКХ Глобал	Приклад
Consent / Згода — Art. 6(1)(a)	Маркетинг, розсилки, фото/відео на заходах, сторітеллінг	Підписка на newsletter через форму на rukh.global, згода на публікацію фото з фестивалю
Contract / Договір — Art. 6(1)(b)	Виконання трудових договорів, договорів ЦПД, волонтерських угод, грантових угод з бенефіціарами	Виплата заробітної плати, нарахування винагороди підрядникам
Legal obligation / Правовий обов'язок — Art. 6(1)(c)	Податкова звітність, обов'язкове соціальне страхування, військовий облік, бухгалтерський облік, звітність донорам	Подача 1ДФ, ЄСВ, фінансовий звіт до донора
Vital interests / Життєво важливі інтереси — Art. 6(1)(d)	Гуманітарні кризові ситуації, медична допомога ВПО	Надання екстреної медичної допомоги бенефіціару

Правова підстава	Коли застосовується в РУКХ Глобал	Приклад
Public task / Публічний інтерес — Art. 6(1)(e)	Рідко — окремі публічні проєкти / advocacy	Публічні звіти, advocacy-кампанії
Legitimate interests / Законний інтерес — Art. 6(1)(f)	Операційні потреби, IT-безпека, fundraising з existing donors	Відеоспостереження в офісі, логування доступів

5.2. Згода (Consent)

5.2.1. Згода повинна бути вільною, конкретною, інформованою, однозначною та виражена ясною дією (opt-in).

5.2.2. Попередньо встановлені галочки (pre-ticked boxes), мовчання або бездіяльність не вважаються згодою.

5.2.3. Організація веде реєстр отриманих згод (Consent Register) — хто, коли, як, на що надав згоду.

5.2.4. Суб'єкт даних має право відкликати згоду у будь-який час. Відкликання оформлюється так само просто, як її надання.

5.2.5. Якщо суб'єкту даних менше 16 років (або нижчий вік, встановлений національним правом), згода надається / підтверджується особою з батьківськими правами.

5.3. Легітимний інтерес та LIA

5.3.1. Перед застосуванням правової підстави «legitimate interests» Організація проводить Legitimate Interests Assessment (LIA), який складається з трьох тестів:

- Purpose test — чи є інтерес законним?
- Necessity test — чи є обробка необхідною?
- Balancing test — чи не переважають інтереси / фундаментальні права суб'єкта даних?

5.3.2. Результати LIA документуються та зберігаються DPO.

6. ОСОБЛИВІ КАТЕГОРІЇ ДАНИХ (ART. 9 GDPR)

6.1. Обробка особливих категорій даних заборонена, окрім випадків, передбачених Art. 9(2) GDPR, зокрема:

- явна згода (explicit consent) суб'єкта даних;
- необхідність для виконання обов'язків у сфері трудового, соціального права;
- захист життєво важливих інтересів суб'єкта, якщо суб'єкт не здатний надати згоду;
- обробка у межах законної діяльності некомерційних організацій з політичними, філософськими, релігійними чи профспілковими цілями — лише щодо членів / колишніх членів / осіб, які мають регулярний контакт з організацією;
- дані, свідомо оприлюднені суб'єктом;
- встановлення, здійснення або захист правових вимог;
- істотний публічний інтерес.

6.2. Особливо чутливі категорії для РУКХ Глобал:

- дані про здоров'я (бенефіціари програм арт-терапії, реабілітації ветеранів);
- дані про етнічне походження (українська діаспора, ВПО);
- політичні погляди (учасники advocacy-кампаній);
- дані про дітей (у проєктах Creative Europe, Erasmus+ з дитячою участю).

6.3. При обробці даних ВПО, дітей та інших вразливих груп застосовуються додаткові заходи захисту (safeguarding, приховане зберігання прізвищ у звітах, використання pseudonym-IDs).

7. КАТЕГОРІЇ СУБ'ЄКТІВ ДАНИХ

7.1. Організація обробляє персональні дані наступних категорій суб'єктів:

Категорія	Приклади
Штатні працівники	Керівництво, менеджери проєктів, комунікаційна команда, фінансисти
Особи за договорами ЦПД / підряду	Тренери, коучі, дизайнери, перекладачі, IT-підрядники
Волонтери	Учасники волонтерських програм в Україні та за кордоном
Бенефіціари програм	ВПО, ветерани, учасники реабілітаційних програм, молодь-діаспора
Партнери	Представники партнерських НГО, державних органів, міжнародних організацій
Донатори (приватні особи)	Фізособи, які здійснюють пожертви
Учасники заходів	Учасники конференцій, фестивалів, семінарів
Підписники розсилок	Особи, що підписані на newsletter rukh.global
Кандидати на вакансії	CV, мотиваційні листи
Користувачі цифрових платформ	Зареєстровані користувачі мобільного застосунку, вебсайту
Члени Організації	Дійсні та асоційовані члени згідно зі Статутом (п. 4.2)

8. КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ

8.1. Організація обробляє такі категорії даних (обсяг залежить від категорії суб'єкта та правової підстави):

Категорія даних	Приклади
Ідентифікаційні	ПІБ, дата народження, РНОКПП (ІПН), паспортні дані, номер посвідчення водія
Контактні	Адреса, телефон, email, месенджери, соцмережі
Професійні / HR	Посада, резюме, освіта, досвід, трудова книжка, військовий облік
Фінансові	Банківський рахунок, IBAN, податкова інформація, історія виплат
Онлайн / технічні	IP-адреса, cookies, браузер, пристрій, геолокація, логи
Медіа	Фото, відео, аудіозаписи із заходів
Особливі категорії	Дані про здоров'я (для бенефіціарів), політичні погляди, етнічне походження
Договірні / проєктні	Статус бенефіціара, участь у проєкті, результати участі

9. ДЖЕРЕЛА ОТРИМАННЯ ДАНИХ

9.1. Організація отримує персональні дані з таких джерел:

- безпосередньо від суб'єкта даних (заявки, реєстраційні форми, анкети, договори, email-комунікація);
- публічні реєстри та відкриті джерела (реєстр юросіб, офіційні сайти);
- від партнерських організацій — виключно на підставі укладених угод про обмін даними / DPA, за наявності правової підстави у партнера;
- від публічних органів (посольства, консульства — у разі обробки даних ВПО, біженців);
- автоматично (cookies, analytics, server logs — з повідомленням та за наявності згоди, якщо потрібно).

9.2. При отриманні даних не від суб'єкта Організація у розумний строк, але не пізніше 30 днів (Art. 14 GDPR), надає суб'єкту Privacy Notice з інформацією про джерело.

10. ПЕРЕДАЧА ДАНИХ ТРЕТІМ ОСОБАМ

10.1. Передача процесорам

10.1.1. Організація залучає процесорів (хмарні сервіси, бухгалтерські та юридичні підрядники, email-платформи, CRM) лише на підставі укладеного Договору про обробку персональних даних (Data Processing Agreement, DPA) — див. Додаток В.

10.1.2. DPA укладається відповідно до Art. 28 GDPR та містить обов'язкові елементи: предмет, тривалість, характер, мета обробки, тип даних, категорії суб'єктів, обов'язки та права Контролера.

10.1.3. Залучення субпроцесорів (sub-processors) процесором дозволяється тільки з попередньої письмової згоди Контролера.

10.2. Передача партнерам

10.2.1. Передача даних партнерам у рамках спільних проєктів здійснюється на підставі:

- Grant Agreement / Consortium Agreement з донором (який дозволяє обмін даними між партнерами);
- окремої DPA або Data Sharing Agreement;
- у моделі joint controllers (Art. 26 GDPR) — додатково з Joint Controllership Agreement.

10.3. Передача донорам та публічним органам

10.3.1. Звітність донорам (ЄС, ООН-агенції, GIZ, SIDA) здійснюється на підставі Grant Agreement. Організація за замовчуванням передає агреговані / знеособлені дані; персональні дані передаються лише у випадку, якщо це прямо передбачено Grant Agreement.

10.3.2. Передача публічним органам здійснюється виключно на підставі письмового запиту з посиланням на закон.

10.4. Транскордонна передача

10.4.1. Передача в межах Європейського економічного простору (EEA) здійснюється вільно.

10.4.2. Передача з України до ЄС. Станом на 2026 рік Єврокомісія не прийняла загальної adequacy decision щодо України; передача здійснюється на підставі Art. 49 GDPR (derogations) або SCCs.

10.4.3. Передача за межі EEA (США, Велика Британія, інші) здійснюється на одній із підстав:

- adequacy decision Єврокомісії (наприклад, UK adequacy decision, EU-US Data Privacy Framework);
- Standard Contractual Clauses (SCCs) 2021/914;
- Binding Corporate Rules (BCRs);
- derogations Art. 49 (явна згода, необхідність для виконання договору тощо).

10.4.4. Перед транскордонною передачею проводиться Transfer Impact Assessment (TIA).

11. СТРОКИ ЗБЕРІГАННЯ (RETENTION)

11.1. Строки зберігання персональних даних визначаються відповідно до цілей обробки, вимог законодавства та донорських вимог. Загальна таблиця — Додаток И.

Категорія	Строк зберігання	Підстава
Особові справи працівників	75 років	Перелік типових документів Мін'юсту, 2021
Первинні кадрові документи (табелі, графіки)	5 років	Законодавство України
Бухгалтерські первинні документи	3 роки (загальний) / 5 років (п. 44.3 ПКУ)	ПКУ, ЗУ 996-XIV
Банківські виписки, договори з донорами	7-10 років	Грантові угоди
Дані підписників marketing розсилок	До відкликання згоди + 1 рік (архів)	Consent withdrawal
Заявки на вакансії (неприйняті)	6 місяців (з явної згоди — до 1 року)	Практика ЄС
Проєктні дані (ЄС-гранти)	10 років після закриття проєкту	EU Financial Regulation 2024/2509
Cookies (сесійні)	До закриття браузера	ePrivacy
Cookies (аналітика)	13-26 місяців	Cookie Policy
Логи IT-систем	12 місяців	IT-безпека
Відеоспостереження в офісі	30 днів	Legitimate interest
Data Breach Register	5 років	Accountability
Consent Register	Строк зберігання даних + 3 роки	Accountability
DSAR Register	3 роки після виконання запиту	Accountability

11.2. Знищення та знеособлення

11.2.1. Після закінчення строку зберігання дані знищуються безповоротно або знеособлюються (pseudonymization / anonymization).

11.2.2. Знищення фізичних носіїв оформлюється Актом знищення, підписаним DPO та відповідальним працівником.

11.2.3. Для цифрових носіїв застосовується cryptoshredding (знищення ключів шифрування) або secure wipe за стандартом NIST SP 800-88.

11.2.4. Знищення даних у хмарних сервісах ініціюється шляхом видалення та підтверджується процесором.

12. ПРАВА СУБ'ЄКТІВ ДАНИХ

12.1. Суб'єкти даних мають такі права згідно з Art. 15-22 GDPR та ст. 8 ЗУ № 2297-VI:

Право	Опис
Право на інформацію (Art. 13-14)	Отримати Privacy Notice при зборі даних
Право доступу (Art. 15)	Отримати копію даних та інформацію про обробку
Право на виправлення (Art. 16)	Вимагати виправлення неточних даних
Право на видалення / бути забутим (Art. 17)	Вимагати видалення при відсутності підстав для подальшої обробки
Право на обмеження обробки (Art. 18)	Вимагати тимчасового обмеження обробки
Право на портативність (Art. 20)	Отримати дані у структурованому форматі (JSON, CSV) та передати іншому контролеру
Право на заперечення (Art. 21)	Заперечувати обробку на підставі legitimate interests або прямий маркетинг
Право не бути об'єктом автоматизованого рішення (Art. 22)	У т.ч. щодо профілювання, що має правові наслідки
Право подати скаргу	До Уповноваженого ВРУ з прав людини або до наглядового органу ЄС (DPA) у країні проживання

12.2. Процедура подання та розгляду запитів (DSAR)

12.2.1. Суб'єкт даних подає запит через:

- email: privacy@rukh.global (основний канал);
- онлайн-форму на rukh.global/privacy;
- паперовий лист на юридичну адресу Організації.

12.2.2. Форма запиту — Додаток Д. Вільна форма також приймається.

12.2.3. DPO верифікує особу заявника (через копію документа, підтвердження email, контрольні запитання).

12.2.4. Відповідь надається протягом 30 календарних днів від отримання запиту. У складних випадках строк може бути продовжено ще на 60 днів з письмовим обґрунтуванням.

12.2.5. Відповідь надається у тому самому форматі, у якому подано запит, або у запитуваному форматі.

12.2.6. Послуги безкоштовні. Плата може стягуватися лише за явно необґрунтовані або повторні запити.

12.2.7. У разі відмови DPO обґрунтовує рішення та інформує про право оскарження до наглядового органу та суду.

12.2.8. Усі запити фіксуються в реєстрі DSAR (Data Subject Access Requests Register).

13. DPIA — ОЦІНКА ВПЛИВУ НА ЗАХИСТ ДАНИХ

13.1. DPIA (Data Protection Impact Assessment) проводиться ОБОВ'ЯЗКОВО перед початком обробки, якщо обробка може становити високий ризик для прав і свобод суб'єктів (Art. 35 GDPR). Зокрема:

- систематичний та екстенсивний моніторинг поведінки (веб-трекінг, CCTV, location tracking);
- великомасштабна обробка особливих категорій даних (здоров'я, політичні погляди);

- систематична обробка даних публічно доступних зон;
- впровадження нових технологій (AI, big data, biometrics);
- обробка даних вразливих груп (діти, ВПО, особи з інвалідністю);
- профілювання, яке приводить до правових наслідків.

13.2. Приклади, коли DPIA необхідна для РУКХ Глобал:

- впровадження нового мобільного застосунку зі збором геолокації діаспори;
- аналіз поведінки користувачів на платформі з AI-рекомендаціями;
- обробка медичних даних ветеранів у програмах арт-терапії;
- CCTV-відеоспостереження у місцях проведення заходів.

13.3. Структура DPIA (Додаток Г):

- систематичний опис процесу обробки, цілі;
- оцінка необхідності та пропорційності;
- ідентифікація ризиків для прав і свобод;
- заходи зменшення ризиків.

13.4. Якщо після DPIA залишковий ризик залишається високим, Організація проводить prior consultation з Уповноваженим ВРУ (в Україні) або наглядовим органом ЄС (Art. 36).

14. PRIVACY BY DESIGN & BY DEFAULT

14.1. Організація впроваджує принципи Privacy by Design та Privacy by Default (Art. 25 GDPR) на всіх етапах розробки продуктів, процесів та партнерств.

14.2. Privacy by Design:

- захист персональних даних враховується ще на етапі проєктування IT-системи / процесу;
- мінімізація даних, pseudonymisation, шифрування впроваджуються на технологічному рівні.

14.3. Privacy by Default:

- за замовчуванням обробляються лише дані, необхідні для конкретної мети;
- усі privacy-налаштування на цифрових платформах РУКХ Глобал за замовчуванням встановлюються на максимальний рівень захисту;
- дані не є публічно доступними без активної дії суб'єкта.

15. ТЕХНІЧНІ ТА ОРГАНІЗАЦІЙНІ ЗАХОДИ (TOMs)

15.1. Організація впроваджує комплекс технічних та організаційних заходів (Art. 32 GDPR) для забезпечення безпеки обробки, адекватних ризикам. Чек-лист TOMs — Додаток Ж.

15.2. Технічні заходи

- шифрування даних at rest (диски, бази даних) та in transit (HTTPS/TLS 1.3);
- багатофакторна автентифікація (MFA) для всіх облікових записів з доступом до персональних даних;
- централізоване керування доступами (Identity & Access Management), роль-базований доступ (RBAC);
- backup & disaster recovery — не рідше ніж раз на 24 години, з тестовим відновленням раз на квартал;
- логування доступу, зміни, видалення даних;
- антивірусний захист, EDR, автоматичне оновлення ОС та ПЗ;
- сегментація мережі, VPN для віддаленого доступу;
- pseudonymisation / анонімізація у звітах, dashboards, дослідженнях;
- data loss prevention (DLP) для чутливих каналів.

15.3. Організаційні заходи

- призначений DPO (п. 17);

- політика чистого столу та чистого екрану;
- NDA для всіх працівників, підрядників, волонтерів;
- навчання (onboarding + щорічний refresh);
- процедура onboarding/offboarding працівників з обліком доступів;
- періодичний аудит (раз на рік) та penetration testing (раз на 2 роки).

16. COOKIES ТА ЕЛЕКТРОННИЙ МАРКЕТИНГ

16.1. На сайті rukh.global застосовується cookie consent banner, що відповідає вимогам ePrivacy Directive та GDPR.

16.2. Cookies класифіковано за категоріями:

- strictly necessary — без згоди;
- performance / analytics — за попередньою згодою (opt-in);
- marketing / advertising — за попередньою згодою;
- functional — за попередньою згодою.

16.3. Повна інформація — у Cookie Policy (Додаток 3), доступній на сторінці rukh.global/cookies.

16.4. Email-маркетинг (newsletters) здійснюється лише за явною opt-in згодою. Кожен лист містить кнопку unsubscribe.

17. DATA PROTECTION OFFICER (DPO)

17.1. Організація призначає Data Protection Officer (DPO) — відповідно до Art. 37-39 GDPR. Для РУКХ Глобал призначення DPO є рекомендованим (за масштабом обробки, у т.ч. особливих категорій даних бенефіціарів, та моніторингом поведінки через digital platforms).

17.2. Кваліфікаційні вимоги до DPO

- експертне знання законодавства про захист персональних даних (GDPR, ЗУ 2297-VI);
- досвід роботи у сфері compliance / data protection від 3 років;
- сертифікація (CIPP/E, CIPM, ISO 27701 Lead Implementer — бажано);
- володіння українською та англійською мовами.

17.3. Форми призначення

- внутрішній DPO — штатний працівник, без конфлікту інтересів (не може бути керівником IT, HR, фінансів);
- зовнішній DPO — за договором ЦПД з юридичною / фізичною особою.

17.4. Функції DPO

- інформування та консультування Контролера та працівників про зобов'язання;
- моніторинг відповідності (compliance);
- консультування щодо DPIA;
- співпраця з Уповноваженим ВРУ та наглядовими органами ЄС;
- контактна особа для суб'єктів даних;
- ведення ROPA, DSAR Register, Breach Register, Consent Register.

17.5. Контакт DPO: privacy@rukh.global.

17.6. DPO звітує безпосередньо виконавчому директору та Голові Правління.

18. ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ (DATA BREACH)

18.1. Data breach (порушення безпеки персональних даних) — порушення, що призводить до випадкового / незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних.

18.2. Процедура реагування (повний Response Plan — Додаток Є)

18.2.1. Крок 1 (T+0 год): виявлення → негайне інформування DPO та IT-адміністратора.

18.2.2. Крок 2 (T+0-24 год): containment — ізоляція уражених систем, зупинка витоку.

18.2.3. Крок 3 (T+0-48 год): assessment — масштаб, категорії даних, кількість суб'єктів, імовірні наслідки.

18.2.4. Крок 4 (T+0-72 год): notification:

- повідомлення Уповноваженому ВРУ з прав людини (в Україні) та/або наглядовому органу ЄС (за lead supervisory authority) ПРОТЯГОМ 72 ГОДИН з моменту виявлення;
- якщо порушення несе високий ризик для прав суб'єктів — невідкладне повідомлення самим суб'єктам (Art. 34 GDPR);
- якщо повідомлення за 72 год неможливе — письмове обґрунтування затримки.

18.2.5. Крок 5: remediation — усунення причин, відновлення.

18.2.6. Крок 6: post-incident review — аналіз, висновки, оновлення TOMs.

18.3. Вміст повідомлення регулятору

- характер порушення, категорії та приблизна кількість суб'єктів і записів;
- контакт DPO;
- ймовірні наслідки;
- вжиті / запропоновані заходи.

18.4. Breach Register

DPO веде Breach Register з усіма інцидентами (у т.ч. тими, що не потребували повідомлення), зі строком зберігання 5 років.

19. ПІДРЯДНИКИ ТА POST-EMPLOYMENT ЗОБОВ'ЯЗАННЯ

19.1. Усі працівники, особи за ЦПД, волонтери та підрядники підписують Угоду про нерозголошення (NDA), яка включає положення про конфіденційність персональних даних.

19.2. Зобов'язання зберігати конфіденційність зберігаються БЕЗСТРОКОВО після припинення трудових / договірних відносин.

19.3. При припиненні відносин працівник зобов'язаний повернути всі носії з персональними даними, видалити дані зі своїх особистих пристроїв (BYOD).

19.4. Проводиться offboarding-процедура: скасування всіх доступів протягом 24 годин, ротація ключів / паролів.

20. НАВЧАННЯ ПЕРСОНАЛУ

20.1. Організація забезпечує обов'язкове навчання з захисту персональних даних для всіх осіб, які мають доступ до даних.

20.2. Формат навчання:

- Induction — протягом перших 14 днів після працевлаштування / початку волонтерства;
- Щорічне оновлення (refresh) — один раз на календарний рік;
- Цільові тренінги після критичних інцидентів / змін в законодавстві.

20.3. Зміст навчання:

- принципи GDPR та ЗУ 2297-VI;
- правила збору, обробки, зберігання, передачі даних;

- права суб'єктів та порядок обробки DSAR;
- data breach — процедура реагування;
- технічні правила (passwords, MFA, phishing-awareness).

20.4. Після навчання працівник складає тест та підписує підтвердження. Облік веде HR / DPO.

21. РЕЄСТРИ

21.1. Організація веде наступні обов'язкові реєстри:

Реєстр	Опис
ROPA (Art. 30 GDPR)	Реєстр усіх процесів обробки (хто, які дані, для чого, підстава, retention, передача). Шаблон — Додаток Е.
Consent Register	Реєстр отриманих згод: хто, коли, на що, канал, версія формулювання
DSAR Register	Реєстр запитів суб'єктів даних
Breach Register	Реєстр інцидентів безпеки
LIA Register	Реєстр проведених Legitimate Interests Assessment
DPIA Register	Реєстр проведених оцінок впливу на захист даних
TIA Register	Реєстр Transfer Impact Assessments
Training Log	Облік проходження навчань
Vendor/DPA Register	Облік процесорів та укладених DPA

21.2. Усі реєстри ведуться DPO в електронному вигляді з контролем версій.

21.3. Реєстри надаються Уповноваженому ВРУ / наглядовому органу ЄС на запит.

22. ВІДПОВІДАЛЬНІСТЬ

22.1. Контролер (ГО «РУКХ Глобал») несе загальну відповідальність за дотримання цього Положення та законодавства про захист персональних даних.

22.2. Голова Правління:

- затверджує Положення та суттєві зміни;
- забезпечує ресурси для реалізації Положення.

22.3. Виконавчий директор:

- забезпечує операційне впровадження;
- призначає DPO;
- затверджує пов'язані процедури.

22.4. DPO:

- координує імплементацію;
- веде реєстри, проводить DPIA, навчає персонал;
- контактна особа для суб'єктів даних та регуляторів.

22.5. Кожен працівник / волонтер / підрядник відповідає за дотримання Положення у межах своїх обов'язків.

22.6. За порушення законодавства про захист персональних даних передбачено:

- дисциплінарну, цивільну, адміністративну (ст. 188-39, 188-40 КУпАП) та кримінальну (ст. 182 ККУ) відповідальність за українським правом;
- адміністративні штрафи згідно з GDPR — до 20 млн євро або 4% річного світового обороту (для Організацій найвища межа);
- цивільні позови суб'єктів даних про відшкодування збитків.

23. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

23.1. Положення набирає чинності з моменту затвердження Правлінням ГО «РУКХ Глобал» та підписання Головою Правління.

23.2. Положення переглядається не рідше одного разу на 2 роки або при:

- суттєвих змінах у законодавстві України чи праві ЄС;
- суттєвих змінах діяльності Організації;
- значних інцидентах (data breach);
- рекомендаціях аудитів донорів.

23.3. Зміни до Положення затверджуються Правлінням.

23.4. З моменту набрання чинності всі попередні внутрішні документи, що суперечать цьому Положенню, втрачають чинність у відповідній частині.

23.5. Оригінал підписаного Положення зберігається в DPO / юридичному відділі. Актуальна версія публікується на внутрішньому порталі та за запитом надається персоналу.

23.6. Відповідальний за Положення: DPO ГО «РУКХ Глобал» — privacy@rukh.global.

ДОДАТОК A. PRIVACY NOTICE (шаблон)

Для: працівників / волонтерів / бенефіціарів / учасників заходів (адаптувати за потреби)

1. Хто ми

Контролер персональних даних: Громадська організація «РУКХ Глобал», юридична адреса: Україна, с-ще Гостомель. Контакт: hello@rukh.global. DPO: privacy@rukh.global.

2. Які дані ми обробляємо

[Зазначити конкретні категорії: ПІБ, email, телефон, фото, IBAN тощо]

3. З якою метою

[Наприклад: виконання трудового договору; направлення newsletter; реалізація грантового проєкту XYZ, фінансованого Creative Europe]

4. Правова підстава

[Art. 6(1)(b) — договір / Art. 6(1)(a) — згода / Art. 6(1)(c) — правовий обов'язок / Art. 6(1)(f) — legitimate interest]

5. Кому ми передаємо дані

[Конкретні категорії отримувачів: банк, податкова, донор, хмарний провайдер Google Workspace (ЄС/США на підставі EU-US DPF)]

6. Скільки зберігаємо

[Строк зберігання — з посиланням на Retention Schedule]

7. Транскордонна передача

[Країни поза EEA, підстава: SCCs / adequacy decision]

8. Ваші права

Ви маєте права доступу, виправлення, видалення, обмеження обробки, портативності, заперечення, відкликання згоди, подання скарги до Уповноваженого ВРУ з прав людини або наглядового органу ЄС у країні проживання.

9. Як звернутися

Email: privacy@rukh.global. Відповідь — протягом 30 днів.

ДОДАТОК Б. ФОРМА ЗГОДИ (CONSENT FORM)

Я, _____ (ПІБ), надаю свою вільну, конкретну, інформовану, однозначну згоду ГО «РУКХ Глобал» (Контролер) на обробку моїх персональних даних з наступними цілями (позначте обране):

☐ 1. Отримання email-розсилки новин РУКХ Глобал

☐ 2. Публікація моїх фото / відео, зроблених на заходах Організації, у соцмережах, на сайті, у звітах донорам

☐ 3. Передача моїх даних партнерам Організації у межах конкретного проєкту: _____

☐ 4. Обробка особливих категорій даних (здоров'я) у межах програми _____ (якщо застосовно)

☐ 5. Передача моїх даних за межі ЄЕЗ (до США / інших країн) на підставі SCCs

Я поінформований(а) про право відкликати згоду в будь-який час шляхом звернення на privacy@rukh.global без негативних наслідків, а також про всі інші права суб'єкта даних згідно зі ст. 15-22 GDPR.

Дата: _____ Підпис: _____ Ім'я друкованими: _____

Службова частина: Отримав: _____ Канал отримання: □ online form □ email □ paper Версія формулювання: v1.0

ДОДАТОК В. DATA PROCESSING AGREEMENT (DPA) — СТИСЛИЙ ШАБЛОН

Укладається між ГО «РУКХ Глобал» (Контролер) та _____ (Процесор) відповідно до Art. 28 GDPR.

1. Предмет та тривалість

Процесор обробляє персональні дані від імені Контролера у межах надання послуг за основним Договором № ___ від ___.

2. Характер і мета обробки [Вказати: наприклад, хостинг даних, обробка платежів, email-розсилки]

3. Типи даних та категорії суб'єктів

[ПІБ, email, телефон; працівники, бенефіціари тощо]

4. Обов'язки Процесора (Art. 28(3) GDPR)

- обробляти дані лише за документальними інструкціями Контролера;
- забезпечити конфіденційність осіб, які мають доступ до даних;
- вжити усіх необхідних заходів безпеки (Art. 32);
- залучати субпроцесорів лише за попередньою письмовою згодою;
- сприяти Контролеру у виконанні запитів суб'єктів даних;
- сприяти у DPIA та prior consultation;
- повідомляти про data breach протягом 24 годин з моменту виявлення;
- після закінчення послуг — видалити / повернути дані за вибором Контролера;
- надавати доступ до інформації та проведення аудитів.

5. Субпроцесори

Перелік субпроцесорів, попередньо затверджених: _____

6. Транскордонна передача. Передача за межі ЄЕЗ — на підставі SCCs 2021/914 Module ___.

7. Термін дії та припинення

DPA діє протягом строку основного Договору. Зобов'язання щодо конфіденційності — безстрокові.

Дата: _____ За Контролера: _____ За Процесора: _____

ДОДАТОК Г. DPIA TEMPLATE (скорочений)

Розділ	Опис
1. Назва процесу / проєкту	
2. Опис обробки	Потоки даних, системи, категорії суб'єктів, дані, цілі
3. Правова підстава	
4. Необхідність і пропорційність	Чи можна досягти мети з меншим обсягом / менш ризиковими засобами?
5. Консультація стейкхолдерів	Чи опитано суб'єктів даних / DPO / партнерів?
6. Аналіз ризиків	Ідентифікація загроз, ймовірність, наслідки для прав суб'єктів
7. Заходи зменшення ризиків	TOMs, pseudonymisation, навчання, контракти
8. Залишковий ризик	Низький / Середній / Високий
9. Необхідність prior consultation	Так / Ні
10. Підписи	DPO: _____ Дата: _____ Відповідальний за процес: _____

ДОДАТОК Д. DSAR ФОРМА (Data Subject Access Request)

До ГО «РУКХ Глобал», DPO — privacy@rukh.global

Я, _____ (ПІБ), ідентифікатор (email/телефон): _____, прошу (позначте обране):

- надати доступ до моїх персональних даних (Art. 15 GDPR);
- виправити неточні дані (Art. 16): _____;
- видалити мої персональні дані (Art. 17);
- обмежити обробку (Art. 18);
- надати мої дані у структурованому форматі (Art. 20);
- припинити обробку на підставі моїх прав (Art. 21);
- інше: _____.

Підстава / деталі: _____

Бажаний канал відповіді: □ email □ паперова пошта

Додаю документ, що посвідчує особу (копія паспорта — для верифікації): □ так

Дата: _____ Підпис: _____

Службова частина (DPO):

Отримано: _____ ID запиту: _____ Верифікація: □ успішна □ неуспішна Дата відповіді: _____ Результат: _____

ДОДАТОК Е. ROPA — ШАБЛОН РЕЄСТРУ (Art. 30 GDPR)

Процес	Мета	Правова підстава	Категорії суб'єктів та даних	Retention	Отримувачі / передача
HR — трудові відносини	Виконання договору, податки	Art. 6(1)(b), (c)	Працівники: ПІБ, паспорт, РНОКПП, IBAN	75 р. / 5 р.	Банк, ДПС, ПФУ
Volunteer management	Координація волонтерів	Art. 6(1)(b)	Волонтери: ПІБ, email, телефон	Період + 3 р.	Project partners (DPA)
Email newsletter	Маркетинг	Art. 6(1)(a)	Підписники: email, ім'я	До opt-out + 1 р.	Mailchimp / Brevo
Beneficiary register	Реалізація програми	Art. 6(1)(b), 9(2)(g)	Бенефіціари: ПІБ, статус ВПО, здоров'я	10 р. після закриття проєкту	Donor (звіти)
Website analytics	Покращення сайту	Art. 6(1)(a) / (f)	Відвідувачі: IP, cookies	26 міс.	Google (EU-US DPF)

ДОДАТОК Є. DATA BREACH RESPONSE PLAN (step-by-step)

Крок	Час (T = виявлення)	Дія	Відповідальний
1	T + 0 год	Виявлення та негайне інформування DPO та IT	Будь-який працівник → DPO, IT
2	T + 0-2 год	Containment: ізоляція систем, блокування облікових записів, ротація ключів	IT + DPO
3	T + 2-24 год	Assessment: що саме, які дані, скільки суб'єктів, який ризик	DPO + IT
4	T + 24-48 год	Класифікація ризику: низький / середній / високий	DPO
5	T + 48-72 год	Notification — Уповноважений ВРУ / наглядовий орган ЄС	DPO
6	T + 0-7 днів	Notification суб'єктам при високому ризику (Art. 34)	DPO + Комунікації
7	T + 1-30 днів	Remediation, оновлення TOMs, комунікація з партнерами	IT + Керівництво
8	T + 30-45 днів	Post-incident review, оновлення Breach Register	DPO

Критерії «високого ризику» для суб'єкта: можливість фінансової шкоди, крадіжки особистості, репутаційної шкоди, розкриття особливих категорій даних.

ДОДАТОК Ж. TOMs CHECKLIST

#	Захід	Статус	Дата перегляду
1	Шифрування дисків (full-disk encryption) — BitLocker / FileVault		
2	TLS 1.3 для всіх комунікацій		
3	MFA для всіх облікових записів з доступом до PII		
4	Password manager на корпоративному рівні		
5	RBAC — ролі та права задокументовані		
6	Регулярні backup + тести відновлення (щокварталу)		
7	Централізоване логування та моніторинг		
8	Антивірус / EDR на всіх пристроях		
9	Автооновлення ОС та ПЗ		
10	VPN для віддаленого доступу		
11	NDA у всіх трудових / ЦПД-договорах		
12	Onboarding / offboarding checklist для доступів		
13	Навчання з GDPR — induction + annual refresh		
14	Політика чистого столу / екрану		
15	Phishing-симуляції (не рідше 2 разів на рік)		
16	Penetration testing (раз на 2 роки)		
17	Інвентаризація систем / даних (раз на рік)		
18	BYOD-політика та MDM		
19	DLP для чутливих каналів		
20	Cookie consent banner на rukh.global		

ДОДАТОК З. COOKIE POLICY (стислий зразок для rukh.global)

1. Ми використовуємо cookies та подібні технології на сайті rukh.global для забезпечення функціональності, аналітики та маркетингу.

2. Категорії cookies:

Категорія	Призначення	Згода	Термін
Strictly necessary	Сесійна автентифікація, безпека	Не потрібна	Session
Performance / Analytics	Google Analytics 4 — статистика відвідувань	Opt-in	13 міс.

Категорія	Призначення	Згода	Термін
Marketing	Meta Pixel, Google Ads — ретаргетинг	Opt-in	26 міс.
Functional	Вибір мови, теми	Opt-in	12 міс.

3. Ви можете змінити або відкликати згоду в будь-який час через cookie banner або Налаштування приватності.

4. Контакт: privacy@rukh.global.

ДОДАТОК И. RETENTION SCHEDULE (розширена таблиця)

Категорія даних	Строк зберігання	Підстава	Примітка
Трудові договори, накази	75 років	Перелік типових документів	Для пенсійного стажу
Особова справа	75 років	Законодавство	
Табелі, графіки, відпустки	5 років	КЗпП, ЗУ 996	
ЦПД-договори	3 роки (з документами оплат — 5)	ЦКУ + ПКУ	
Заявки на вакансії	6 міс. / 12 міс. зі згодою	GDPR practice	
Рекомендаційні листи	6 міс.	Мінімізація	
Бухгалтерські первинні	5 років	ПКУ п. 44.3	
Банківські виписки	5 років	ПКУ	
Звіти донорам ЄС	10 років після закриття проєкту	EU FR 2024/2509	
Грантові угоди USAID / State Dept	10 років	2 CFR 200	
Marketing subscribers	До opt-out + 1 рік	Consent	Архів з мінімізованими даними
Учасники заходів (без згоди на подальший контакт)	1 рік після заходу	Звіти донорам	
Фото / відео заходів	5 років (з згодою) / до відкликання	Consent	
Відеоспостереження	30 днів	Legitimate interest	Циклічне перезапис
IT-логи	12 місяців	Security	
Cookies (analytics)	13-26 місяців	Consent	Залежить від інструменту

Категорія даних	Строк зберігання	Підстава	Примітка
Cookies (strictly necessary)	Session	Art. 6(1)(f)	
Breach Register	5 років	Accountability	
Consent Register	Термін зберігання PII + 3 роки	Accountability	
DSAR Register	3 роки після закриття запиту	Accountability	
DPIA-документи	Період обробки + 3 роки	Accountability	
NDAs	10 років після припинення	Цивільне право	
Статутні документи	Постійно	ЗУ 4572-VI	