

ГО «ПІСЛЯЗАВТРА» / NGO AFTERTOMORROW

ЗВЕДЕНА ПОЛІТИКА ЗАХИСТУ ДАНИХ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ | UNIFIED DATA PROTECTION & INFORMATION SECURITY POLICY

Документ № 08 • Версія 1.2 • Затверджено 2 жовтня 2026 (зміни — 5 жовтня 2026) • Чинна з 5 жовтня 2026 • Наступний перегляд 5 жовтня 2027
Document No. 08 • Version 1.2 • Approved 2 October 2026 (amended 5 October 2026) • Effective 5 October 2026 • Next review 5 October 2027

ЗАТВЕРДЖЕНО / APPROVED

Голова правління / Chair of the Board

Ірина Рубіс / Iryna Rubis

Підпис / Signature: _____

ПІБ / Name: _____

Дата / Date: _____

Затверджено протоколом засідання Правління від 02.10.2026; зміни затверджено протоколом засідання Правління від 05.10.2026 / Approved by the minutes of the Board meeting of 2 October 2026; amendments approved by the minutes of 5 October 2026

ПЕРЕДМОВА / PREAMBLE

ГО «Післязавтра» зареєстрована та здійснює діяльність в Україні. Обробка персональних даних регулюється Законом України «Про захист персональних даних» № 2297-VI (зі змінами) та Конвенцією Ради Європи № 108. Якщо грантова угода з іноземним донором встановлює додаткові вимоги до захисту даних (зокрема GDPR), вони виконуються як договірні зобов'язання за відповідним проектом. Ця Політика встановлює мінімальні стандарти збору, обробки, зберігання та передачі персональних даних у всій діяльності Організації.

NGO AfterTomorrow is registered and operates in Ukraine. Personal data processing is governed by the Law of Ukraine No. 2297-VI on Personal Data Protection (as amended) and Council of Europe Convention No. 108. Where a grant agreement with a foreign donor sets additional data protection requirements (including the GDPR), these are fulfilled as contractual obligations under the respective project. This Policy sets the minimum standards for collecting, processing, storing, and transferring personal data across all organisational activities.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ • 1. GENERAL PROVISIONS

1.1 Сфера застосування

Поширюється на: весь персонал, волонтерів, підрядників, партнерів та правління. Охоплює всі персональні дані, що обробляються Організацією в будь-якому форматі — цифровому або паперовому.

1.1 Scope

Applies to: all staff, volunteers, contractors, partners, and board members. Covers all personal data processed by the Organisation in any format — digital or paper.

1.2 Ролі та відповідальність

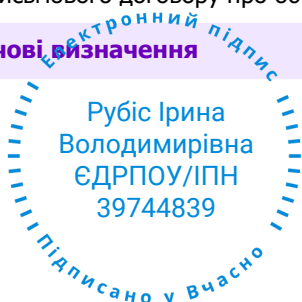
Володілець персональних даних: ГО «Післязавтра». Відповідальна особа з питань захисту персональних даних: Голова правління або призначена особа. Розпорядник персональних даних: будь-який підрядник або партнер, що обробляє дані за дорученням Організації, — виключно на підставі письмового договору про обробку даних.

1.2 Roles & Responsibilities

Personal data owner (controller): NGO AfterTomorrow. Person responsible for personal data protection: the Chair of the Board or a designated person. Personal data processor: any contractor or partner processing data on the Organisation's behalf — solely under a written data processing agreement.

1.3 Ключові визначення

1.3 Key Definitions



- Персональні дані — будь-яка інформація, що стосується ідентифікованої фізичної особи або особи, яку можна ідентифікувати.
- Чутливі дані (Особлива категорія) — дані про расове/етнічне походження, здоров'я, сексуальну орієнтацію, релігію, переконання, біометричні дані.
- Обробка — будь-яка операція з персональними даними.
- Порушення даних — будь-яке порушення безпеки, що призводить до знищення, втрати, зміни або несанкціонованого розкриття персональних даних.

- Personal data — any information relating to an identified or identifiable natural person.
- Special category data — data revealing racial/ethnic origin, health, sexual orientation, religion, beliefs, biometric data.
- Processing — any operation on personal data.
- Data breach — any security incident resulting in destruction, loss, alteration, or unauthorised disclosure of personal data.

2. ПРАВОВІ ПІДСТАВИ ОБРОБКИ • 2. LEGAL BASIS FOR PROCESSING

2.1 Підстави обробки (ст. 11 ЗУ № 2297-VI): згода суб'єкта персональних даних; укладення та виконання правочину, стороною якого є суб'єкт даних (трудові та цивільно-правові договори, угоди з партнерами); виконання обов'язку володільця, передбаченого законом (кадровий облік, податкова та фінансова звітність); захист життєво важливих інтересів суб'єкта; законний інтерес Організації, крім випадків, коли інтереси суб'єкта переважають. 2.2 Чутливі дані (ст. 7 ЗУ № 2297-VI): дані про здоров'я, етнічне походження, релігійні переконання тощо обробляються лише за однозначної згоди суб'єкта або в інших випадках, прямо передбачених ст. 7; про обробку даних, що становить особливий ризик, повідомляється Уповноважений ВРУ з прав людини (ст. 9). Всі формуляри збору чутливих даних містять посилання на цю Політику та Форму згоди (Додаток А).

2.1 Legal bases (Art. 11 of Law No. 2297-VI): consent of the data subject; conclusion and performance of a transaction to which the data subject is a party (employment and civil-law contracts, partner agreements); compliance with a legal obligation of the data owner (HR records, tax and financial reporting); protection of the data subject's vital interests; legitimate interest of the Organisation, except where the data subject's interests prevail. 2.2 Sensitive data (Art. 7 of Law No. 2297-VI): data on health, ethnic origin, religious beliefs, etc. is processed only with the data subject's unambiguous consent or in other cases expressly provided by Art. 7; processing posing a special risk is notified to the Ukrainian Parliament Commissioner for Human Rights (Art. 9). All forms collecting sensitive data reference this Policy and the Consent Form (Annex A).

Обробка персональних даних в Україні здійснюється відповідно до Закону від 01.06.2010 № 2297-VI зі змінами. Основні вимоги:

- реєстрація баз персональних даних (якщо вимагається);
- мета обробки чітко визначена та обмежена;
- термін зберігання не перевищує необхідного;
- особи мають право на доступ, виправлення та видалення.

Processing of personal data in Ukraine follows Law No. 2297-VI of 01.06.2010 as amended. Key requirements:

- registration of personal data bases (where required);
- purpose clearly defined and limited;
- retention period does not exceed what is necessary;
- individuals have rights of access, correction, and deletion.

3. ПРАВА СУБ'ЄКТІВ ДАНИХ • 3. DATA SUBJECT RIGHTS

Кожна особа, чиї дані обробляє Організація, має права, визначені ст. 8 ЗУ № 2297-VI, зокрема: отримати доступ до своїх даних та інформацію про мету обробки; вимагати виправлення неточних даних; вимагати видалення даних, якщо вони обробляються незаконно чи є недостовірними; заперечувати проти обробки; відкликати згоду в будь-який момент; звертатися зі скаргами до Уповноваженого ВРУ з прав людини або до суду. Запити подаються на welcome@aftertomorrow.org. Строк відповіді: 30 календарних днів (ст. 16–17 ЗУ № 2297-VI). Скарги: Уповноважений ВРУ з прав людини — ombudsman.gov.ua.

Every individual whose data the Organisation processes has the rights defined by Art. 8 of Law No. 2297-VI, including: to know about the processing and location of their data; to access their data and information on the purpose of processing; to demand rectification of inaccurate data; to demand erasure of data processed unlawfully or found inaccurate; to object to processing; to withdraw consent at any time; to lodge complaints with the Ukrainian Parliament Commissioner for Human Rights or a court.

Requests: welcome@aftertomorrow.org. Response deadline: 30 calendar days (Arts. 16–17 of Law No. 2297-VI). Complaints: Ukrainian Parliament Commissioner for Human Rights — ombudsman.gov.ua.

4. ЗАХОДИ БЕЗПЕКИ ДАНИХ • 4. DATA SECURITY MEASURES

4.1 Технічні заходи

4.1 Technical Measures

- Шифрування даних у спокої та при передачі (TLS 1.2+).
- Двофакторна автентифікація для всіх корпоративних систем.
- Регулярне резервне копіювання (мінімум щотижня).
- Обмежений доступ за принципом мінімальних привілеїв.
- Захист пристроїв: антивірус, оновлення ОС, шифрування дисків.

- Encryption of data at rest and in transit (TLS 1.2+).
- Two-factor authentication for all organisational systems.
- Regular backups (minimum weekly).
- Access restrictions based on least-privilege principle.
- Device protection: antivirus, OS updates, disk encryption.

4.2 Організаційні заходи

- Обов'язковий інструктаж з захисту даних при прийомі на роботу та щорічно.
- Угода про конфіденційність підписується кожним членом персоналу та волонтером.
- Перевірка підрядників: DPA до початку обробки даних.
- Паперові записи зберігаються у замкнених шафах.
- Доступ до персональних справ — лише для уповноважених осіб.

4.2 Organisational Measures

- Mandatory data protection briefing at onboarding and annually.
- Confidentiality agreement signed by every staff member and volunteer.
- Vendor due diligence: DPA required before data processing begins.
- Paper records kept in locked cabinets.
- Access to personal files restricted to authorised persons only.

5. ТЕРМІНИ ЗБЕРІГАННЯ ДАНИХ • 5. DATA RETENTION SCHEDULE

Категорія даних <i>Data Category</i>	Термін зберігання <i>Retention Period</i>	Місце зберігання <i>Storage Location</i>	Підстава <i>Basis</i>
Закупівельна та фінансова документація (заявки, пропозиції, договори, рахунки, акти) <i>Procurement and financial records (requisitions, bids, contracts, invoices, completion acts)</i>	7 років після завершення проекту або остаточного платежу донора, залежно від того, що настає пізніше; довше — якщо вимагає донор <i>7 years after project completion or the donor's final payment, whichever is later; longer where donor rules require</i>	Хмарне сховище + паперові оригінали <i>Cloud storage + paper originals</i>	Документи № 02, № 05; умови грантів <i>Documents No. 02, No. 05; grant terms</i>

Дані персоналу, волонтерів та учасників програм <i>Staff, volunteer and programme participant data</i>	5 років після завершення співпраці або програми; за грантовим проектом — не менше строку, встановленого грантовою угодою, якщо він довший (для грантів ЄС — як правило, 5 років після остаточного платежу); кадрові документи (особові справи, накази з особового складу, особові картки П-2 тощо) зберігаються протягом строків, встановлених Переліком типових документів (наказ Мін'юсту № 578/5 від 12.04.2012) <i>5 years after end of engagement or programme; for a grant-funded project — not less than the period set by the grant agreement where longer (for EU grants, typically 5 years after the final payment); HR records (personnel files, HR orders, P-2 personnel cards, etc.) are retained for the periods set by the List of Standard Documents (Order of the Ministry of Justice No. 578/5 of 12.04.2012)</i>	Хмарне сховище (зашифровано) <i>Cloud storage (encrypted)</i>	Документ № 13; трудове законодавство <i>Document No. 13; employment law</i>
Записи про скарги <i>Complaints records</i>	5 років з моменту закриття справи <i>5 years from case closure</i>	Хмарне сховище (зашифровано), окремо від особових справ <i>Cloud storage (encrypted), separate from personnel files</i>	Документ № 07 <i>Document No. 07</i>
Safeguarding-інциденти (включно з повідомленнями викривачів щодо SEA/CPP) <i>Safeguarding incident records (incl. whistleblower reports on SEA/CPP)</i>	10 років або до досягнення дитиною 28 років — що настане пізніше <i>10 years or until the child turns 28, whichever is later</i>	Зашифрований реєстр; доступ — Уповноважена особа; Голова правління — в обсязі, потрібному для ухвалення рішення (крім справ щодо неї) <i>Encrypted register; access — Safeguarding Officer; Chair of the Board — to the extent needed to take a decision (except for cases concerning her)</i>	Документ № 06, CPP; умови грантів ЄС <i>Document No. 06, CPP; EU grant conditions</i>
Донорські звіти <i>Donor reports</i>	10 років після завершення проекту <i>10 years after project completion</i>	Захищений архів (цифровий та/або паперовий) <i>Secure archive (digital and/or paper)</i>	Документ № 10 <i>Document No. 10</i>
Розрахункові відомості з оплати праці <i>Payroll statements</i>	75 років <i>75 years</i>	Паперовий та цифровий архів <i>Paper and digital archive</i>	Законодавство України (пенсійне забезпечення); Документ № 02 <i>Ukrainian law (pension purposes); Document No. 02</i>

Дані веб-сайту (cookies, IP) <i>Website data (cookies, IP)</i>	До 26 місяців <i>Up to 26 months</i>	Платформа сайту / аналітика <i>Site platform / analytics</i>	Законний інтерес <i>Legitimate interest</i>
Email-листування <i>Email correspondence</i>	3 роки <i>3 years</i>	Хмарне сховище (зашифровано) <i>Cloud storage (encrypted)</i>	Законний інтерес <i>Legitimate interest</i>
Маркетингові фото та відео <i>Marketing photos and video</i>	До відкликання згоди <i>Until consent withdrawn</i>	Захищена папка з обмеженим доступом; сайт та соцмережі <i>Protected restricted-access folder; website and social media</i>	Згода суб'єкта <i>Data subject consent</i>

Ця таблиця є єдиним джерелом строків зберігання для всіх документів Організації. У разі розбіжності з іншим внутрішнім документом застосовується ця таблиця. Якщо законодавство встановлює довший строк зберігання документа, застосовується строк, встановлений законодавством./This table is the single source of retention periods for all documents of the Organisation. In the event of a discrepancy with any other internal document, this table prevails. Where legislation sets a longer retention period for a document, the statutory period applies.

6. ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ ДАНИХ • 6. DATA BREACH NOTIFICATION

6.1 Внутрішня процедура

- Негайно повідомте Голову правління або відповідального за захист даних (впродовж 4 годин з моменту виявлення).
- Задokumentуйте: тип даних, кількість осіб, ймовірний ризик, вжиті заходи.
- Оцініть ризик: чи є ризик для прав та свобод осіб?

6.1 Internal Procedure

- Notify Chair of the Board or Data Protection Representative immediately (within 4 hours of discovery).
- Document: type of data, number of individuals, likely risk, measures taken.
- Assess risk: is there a risk to rights and freedoms of individuals?

6.2 Повідомлення регуляторів

Уповноважений ВРУ з прав людини: про серйозні порушення захисту даних Організація повідомляє без невинуватності затримки (законодавство України не встановлює фіксованого строку; внутрішній стандарт Організації — 72 години з моменту виявлення). Донори: якщо порушення стосується даних учасників грантового проєкту — повідомлення донора у строки грантової угоди (зазвичай 72 години). Суб'єкти даних: повідомляються без зайвої затримки, якщо порушення створює високий ризик для їхніх прав.

6.2 Regulatory Notification

Ukrainian Parliament Commissioner for Human Rights: the Organisation reports serious data breaches without undue delay (Ukrainian law sets no fixed deadline; the Organisation's internal standard is 72 hours from discovery). Donors: where a breach affects data of grant project participants — donor notification within the grant agreement timelines (typically 72 hours). Data subjects: notified without undue delay where the breach poses a high risk to their rights.

7. ПЕРЕДАЧА ДАНИХ • 7. DATA TRANSFERS

- Персональні дані обробляються та зберігаються в Україні. Використання хмарних сервісів, сервери яких розташовані за кордоном (Google Workspace тощо), допускається лише за наявності договору з постачальником послуг, що містить гарантії захисту даних.

- Передача персональних даних іноземним суб'єктам (донорам, партнерам, підрядникам) здійснюється відповідно до ст. 29 ЗУ «Про захист персональних даних» № 2297-VI — лише за однієї з умов: держава отримувача забезпечує належний захист персональних даних (держави-члени ЄСП та сторони Конвенції Ради Європи № 108 вважаються такими за законом); однозначна згода суб'єкта даних на передачу; необхідність укладення або виконання правочину в інтересах суб'єкта даних; захист життєво важливих інтересів суб'єкта; надання відповідних гарантій щодо невтручання в особисте життя у договорі з отримувачем.

- Донорам передається виключно знеособлена (агрегована) звітність. Персональні дані учасників передаються донору лише за явною згодою суб'єкта та за договором, що містить гарантії захисту.

- Якщо грантова угода з донором вимагає дотримання GDPR або інших іноземних стандартів захисту даних — відповідні вимоги виконуються як договірні зобов'язання за конкретним грантом і не змінюють загального правового режиму цієї Політики.

- Кожна передача персональних даних за кордон документується у реєстрі обробки даних.

- **Personal data is processed** and stored in Ukraine. Cloud services with servers located abroad (Google Workspace, etc.) may be used only under a service agreement containing data protection safeguards.

- Transfer of personal data to foreign parties (donors, partners, contractors) is carried out in accordance with Art. 29 of the Law of Ukraine No. 2297-VI on Personal Data Protection — only where one of the following applies: the recipient state ensures adequate personal data protection (EEA member states and parties to Council of Europe Convention No. 108 are deemed adequate by law); the data subject's unambiguous consent to the transfer; the transfer is necessary to conclude or perform a transaction in the data subject's interest; protection of the data subject's vital interests; appropriate contractual safeguards of non-interference with private life are provided by the recipient.

- Donors receive anonymised (aggregated) reporting only. Participants' personal data is transferred to a donor only with the data subject's explicit consent and under an agreement that includes protective safeguards.

- Where a grant agreement requires compliance with the GDPR or other foreign data protection standards, such requirements are fulfilled as contractual obligations under the specific grant and do not alter the general legal regime of this Policy.

- Every cross-border transfer of personal data is documented in the records of processing activities.

8. ДАНІ ДІТЕЙ • 8. CHILDREN'S DATA

Обробка даних осіб, молодших 18 років, потребує:

- письмової згоди батьків/опікунів (Форма згоди, Додаток Б);
- мінімального збору даних — лише необхідна інформація;
- обмеженого доступу — лише уповноважений персонал;
- особливого режиму зберігання та видалення.

Зберігання фото/відео дітей: тільки за явної згоди і виключно для задокументованих цілей програми.

Посилання: Документ № 06a (Додаток В — Форма батьківської згоди).

Processing data of persons under 18 years requires:

- written consent of parent/guardian (Consent Form, Annex B);
- data minimisation — only necessary information;
- restricted access — authorised staff only;
- special retention and deletion regime.

Photography/video of children: only with explicit consent and for documented programme purposes only. Reference: Document 06a (Annex C — Parental Consent Form).

9. НАВЧАННЯ ТА ВІДПОВІДАЛЬНІСТЬ • 9. TRAINING & ACCOUNTABILITY

- Інструктаж при прийомі на роботу: обов'язковий для всіх.
- Щорічне оновлення: кожного вересня.
- Перевірка знань: після навчання — тест або підтвердження.
- Документація: журнал навчань ведеться відповідальним за захист даних.
- Порушення цієї Політики: дисциплінарна відповідальність відповідно до Документа № 03.

- Onboarding briefing: mandatory for all.
- Annual refresh: each September.
- Knowledge check: post-training test or acknowledgement.
- Documentation: training log maintained by Data Protection Representative.
- Breach of this Policy: disciplinary action per Document 03.

ДОДАТОК А: ФОРМА ІНФОРМОВАНОЇ ЗГОДИ (УЧАСНИКИ ПРОГРАМ) • ANNEX A: INFORMED CONSENT FORM (PROGRAMME PARTICIPANTS)**ПІБ / ім'я (або псевдонім):****Full name / name (or alias):****Дата народження:****Date of birth:****Контактний телефон / email:****Contact phone / email:****Назва програми / заходу:****Programme / activity name:****Дата / місце:****Date / location:****Я надаю згоду на:**

- ☐ Збір та обробку моїх персональних даних з метою участі в програмі.
- ☐ Використання знеособлених даних для звітності та аналізу програми.
- ☐ Фотографування / відеозйомку під час заходу (якщо застосовно).
- ☐ Передачу даних партнерам / донорам (лише для цілей програми).

I consent to:

- ☐ Collection and processing of my personal data for the purpose of programme participation.
- ☐ Use of anonymised data for programme reporting and analysis.
- ☐ Photography / video recording during the activity (if applicable).
- ☐ Transfer of data to partners / donors (for programme purposes only).

Я розумію, що:

- Мої дані зберігаються у безпечних умовах та не передаються третім особам без підстави.
- Я можу відкликати згоду в будь-який момент, написавши на welcome@aftertomorrow.org.
- Відкликання не впливає на мою участь у програмі.
- Строк зберігання: 5 років після завершення програми або довше, якщо цього вимагає грантова угода.

I understand that:

- My data is stored securely and not shared with third parties without grounds.
- I can withdraw consent at any time by writing to welcome@aftertomorrow.org.
- Withdrawal does not affect my participation in the programme.
- Retention period: 5 years after programme completion or longer where the grant agreement requires.

Підпис учасника:**Participant signature:****Дата:****Date:**

ДОДАТОК Б: ФОРМА БАТЬКІВСЬКОЇ ЗГОДИ НА ОБРОБКУ ДАНИХ ДИТИНИ • ANNEX B: PARENTAL CONSENT FORM FOR CHILD DATA

ПІБ дитини: _____

Child's full name: _____

Дата народження дитини:

Child's date of birth: _____

ПІБ батька/матері/опікуна:
_____Parent/guardian full name:
_____Контактний телефон / email:
_____Contact phone / email:
_____Відношення до дитини:
_____Relationship to child:

Назва програми: _____

Programme name: _____

Я надаю дозвіл на:

- ☐ Збір та обробку даних дитини для участі в програмі.
- ☐ Фотографування / відеозйомку дитини під час заходу.
- ☐ Передачу даних дитини партнерам / донорам у знеособленому вигляді.

Підпис батька/матері/опікуна:

Дата: _____

I give permission for:

- ☐ Collection and processing of the child's data for programme participation.
- ☐ Photography / video recording of the child during the activity.
- ☐ Transfer of the child's anonymised data to partners / donors.

Parent/guardian signature:

Date: _____

ДОДАТОК В: ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ ДАНИХ (ВНУТРІШНЯ ФОРМА) • ANNEX C: DATA BREACH NOTIFICATION FORM (INTERNAL)**Дата та час виявлення:****Date and time of discovery:****Хто виявив (ПІБ / посада):****Discovered by (name / role):****Тип даних, що постраждали:****Type of data affected:****Кількість постраждалих осіб (приблизно):****Approximate number of individuals affected:****Опис порушення / Description of breach:****Вжиті заходи (негайно) / Immediate action taken:****Рівень ризику (оцінка)**

- ☐ Низький — мала ймовірність шкоди.
- ☐ Середній — можливий вплив, але не критичний.
- ☐ Високий — серйозна ймовірність шкоди або великий обсяг даних.

Risk Level (assessment)

- ☐ Low — low likelihood of harm.
- ☐ Medium — possible impact, not critical.
- ☐ High — serious likelihood of harm or large volume of data.

Дії, що вимагаються

- ☐ Повідомлення постраждалих осіб.
- ☐ Повідомлення українського регулятора.
- ☐ Документування у Реєстрі інцидентів.

Required Actions

- ☐ Notify affected individuals.
- ☐ Notify Ukrainian regulator.
- ☐ Document in Incident Log.

Підпис відповідального за захист даних:**Data Protection Representative signature:****Дата:****Date:***Наступний перегляд: 5 жовтня 2027 (або раніше у разі змін у законодавстві)**Next review: 5 October 2027 (or earlier if legislation changes)*

Документ підписано у сервісі Вчасно (продовження)

08 Data Protection Policy.pdf

Документ відправлено (3081315900): 19:24 05.10.2026

Документ отримано (3081315900): 19:24 05.10.2026

Відправник документу

Електронний підпис

19:24 05.10.2026

ЄДРПОУ/ІПН: 39744839

Юр. назва: ГРОМАДСЬКА ОРГАНІЗАЦІЯ "ПІСЛЯЗАВТРА"

Власник ключа: Рубіс Ірина Володимирівна

Час перевірки КЕП/ЕЦП: 19:24 05.10.2026

Статус перевірки сертифікату: Сертифікат діє

Серійний номер: 04AF212836405D9904000000D8A92D00D1AFEB00

Тип підпису: удосконалений

Тип сертифікату: кваліфікований