



ЗАТВЕРДЖУЮ

Голова Благодійної Організації
"Міжнародний Благодійний Фонд
"Українська Душа"

Богаченко Н.В.

2023 р.

ПОЛІТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ **Благодійної Організації "Міжнародний Благодійний Фонд** **"Українська Душа"**

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця Політика визначає принципи, порядок збору, обробки, зберігання, передачі та захисту персональних даних у діяльності Благодійної Організації «Міжнародний Благодійний Фонд «Українська Душа» (далі - Організація).

1.2. Політика розроблена відповідно до:

- Закону України «Про захист персональних даних»;
- принципів General Data Protection Regulation (GDPR);
- стандартів міжнародних донорів щодо Data Protection, Safeguarding та Accountability to Affected Populations (AAP).

1.3. Організація визнає захист персональних даних невід'ємною частиною прав людини та зобов'язується забезпечувати їх конфіденційність, цілісність та безпеку.

2. ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Персональні дані - будь-яка інформація, що прямо або опосередковано ідентифікує фізичну особу.

Обробка даних - будь-яка дія або сукупність дій з персональними даними (збір, зберігання, використання, передача, знищення).

Суб'єкт персональних даних - фізична особа, чії дані обробляються.

3. ПРИНЦИПИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Організація у своїй діяльності керується такими принципами:

3.1. Законність та співвідповідність

Обробка персональних даних здійснюється виключно на законних підставах, чесно та з повагою до прав суб'єктів даних.

3.2. Прозорість

Суб'єкти персональних даних інформуються про мету, обсяг, строки та способи обробки їхніх даних у зрозумілій формі.

3.3. Обмеження метою (Purpose Limitation)

Персональні дані збираються лише для чітко визначених, законних і конкретних цілей та не використовуються несумісно з цими цілями.

3.4. Мінімізація даних (Data Minimization)

Організація збирає тільки ті дані, які є необхідними та достатніми для реалізації програм і виконання донорських вимог.

3.5. Точність (Accuracy)

Персональні дані повинні бути точними та актуальними. У разі виявлення помилок вони оперативно виправляються або видаляються.

3.6. Обмеження строків зберігання (Storage Limitation)

Дані зберігаються не довше, ніж це необхідно для досягнення мети обробки або відповідно до вимог донора та законодавства.

3.7. Цілісність та конфіденційність (Integrity and Confidentiality)

Організація застосовує технічні та організаційні заходи для захисту даних від несанкціонованого доступу, втрати, знищення або пошкодження.

3.8. Підзвітність (Accountability)

Організація несе відповідальність за дотримання цієї Політики та може підтвердити відповідність принципам захисту даних перед донорами та контролюючими органами.

3.9. Do No Harm

Обробка персональних даних не повинна створювати ризики для безпеки, гідності або добробуту бенефіціарів.

3.10. Safeguarding та захист вразливих груп

Під час роботи з дітьми, особами з інвалідністю, постраждалими від насильства або іншими вразливими групами застосовується підвищений рівень захисту даних.

4. КАТЕГОРІЇ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ

Фонд може обробляти:

- ідентифікаційні дані (ПІБ, дата народження);
- контактні дані (телефон, електронна пошта, адреса);
- соціально-демографічні дані;
- фінансові дані (у разі виплат допомоги);
- чутливі дані (стан здоров'я, статус ВПО тощо) - лише за наявності законних підстав і додаткових гарантій захисту.

5. ПРАВОВІ ПІДСТАВИ ОБРОБКИ

Обробка здійснюється на підставі:

- письмової або електронної згоди суб'єкта;
- виконання договору або грантової угоди;
- законного інтересу Організації;
- виконання вимог законодавства;
- гуманітарних мандатів міжнародних донорів.

6. МЕТА ОБРОБКИ

- реалізація благодійних програм;
- надання гуманітарної допомоги;
- ведення звітності перед донорами;
- моніторинг та оцінка програм;
- забезпечення safeguarding та безпеки бенефіціарів;
- внутрішнє адміністрування та кадрова робота.

7. ПРАВА СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Суб'єкт має право:

- отримати інформацію про обробку своїх даних;
- доступ до своїх даних;
- вимагати виправлення або оновлення;
- вимагати видалення («право бути забутим»);
- обмежити обробку;
- відкликати згоду;
- подати скаргу до уповноваженого органу.

Запити розглядаються протягом 30 календарних днів.

8. ЗАХОДИ БЕЗПЕКИ

Фонд застосовує:

Технічні заходи:

- парольний захист;
- обмеження доступу до баз даних;
- антивірусне програмне забезпечення;
- шифрування електронних носіїв (за потреби).

Організаційні заходи:

- навчання персоналу;
- обмеження доступу за принципом «need-to-know».

9. ПЕРЕДАЧА ДАНИХ ТРЕТІМ ОСОБАМ

9.1. Передача даних донорам або партнерам здійснюється:

- лише в межах необхідного обсягу;
- з дотриманням принципу мінімізації;
- на підставі угод про захист даних (Data Sharing Agreement / DPA).

9.2. У разі міжнародної передачі даних забезпечується належний рівень захисту відповідно до стандартів GDPR.

10. СТРОКИ ЗБЕРІГАННЯ

Персональні дані зберігаються:

- протягом строку реалізації проєкту;
- відповідно до вимог донорів (зазвичай 3–7 років);
- або до моменту відкликання згоди, якщо інше не передбачено законом.

Після завершення строку зберігання дані підлягають безпечному знищенню або анонімізації.

11. ПОРУШЕННЯ БЕЗПЕКИ ДАНИХ (Data Breach)

11.1. У разі витоку або порушення безпеки даних Організація:

- негайно проводить внутрішнє розслідування;
- документує інцидент;
- повідомляє донора (за вимогою грантової угоди);
- інформує суб'єктів даних, якщо існує високий ризик для їхніх прав і свобод.

12. ВІДПОВІДАЛЬНІСТЬ

Порушення цієї Політики тягне за собою дисциплінарну відповідальність працівників, а в разі необхідності – повідомлення відповідних органів.

13. ПЕРЕГЛЯД ПОЛІТИКИ

Політика переглядається не рідше одного разу на 2 роки або за вимогою донора.

14. ЗАТВЕРДЖЕННЯ

Положення набиратимуть чинності з моменту його підписання керівником Організації.