БЛАГОДІЙНА ОРГАНІЗАЦІЯ
«БЛАГОДІЙНИЙ ФОНД
«ДОБРОБУТ УКРАЇНИ»
ЄДРПОУ 40234987
61018, Україна, м. Харків,
вул. Отакара Яроша, 61-А, к. 10

CHARITABLE ORGANIZATION
«CHARITABLE FOUNDATION
«EUDEMONY OF UKRAINE»
№ 40234987
Otakara Yarosha street 61-A ap. 10 Kharkiv
Ukraine 61018

№15 від 05.08.2025

Н А К А З

Про затвердження Політики захисту персональних даних

З метою встановлення основних правила збору, обробки, зберігання та захисту персональних даних осіб, які взаємодіють з Благодійної організації "Благодійний фонд «Добробут України", а також щодо використання персональних даних Благодійною організацією "Благодійного фонду "Добробут України", керуючись Статутом

НАКАЗУЮ:

1. Затвердити Політику захисту персональних даних Благодійної організації «Благодійного фонду "Добробут України» (додається).
2. Контроль за виконанням даного наказу покласти на Офіцера з моніторингу та оцінки.

Голова Правління **Вікторія ПРЕОБРАЖЕНСЬКА**

З Наказом ознайомлені:

Офіцер з моніторингу та оцінки
Іоанн ПРЕОБРАЖЕНСЬКИЙ

Дата: «05» серня 2025 р.

ЗАТВЕРДЖЕНО
Наказом Голови Правління

БО “БФ «ДОБРОБУТ УКРАЇНИ»
від 05.08.2025 №15

ПОЛІТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ «БЛАГОДІЙНИЙ ФОНД “ДОБРОБУТ УКРАЇНИ»

м. Київ – 2025 рік

tel.+380954152277 https://cfdobrobutua.weblium.site e-mail: info@dobrobutua.org
Р/р UA613515330000026007052221644 в ПАТ КБ «Приват Банк» у м. Київ МФО 351533

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця політика захисту персональних даних (далі - Політика) Благодійної організації «Благодійний фонд “Добробут України”» (далі - Організація) встановлює основні правила збору, обробки, зберігання та захисту персональних даних осіб, які взаємодіють з Організацією.

1.2. Політика поширюється на всіх працівників, представників та осіб, які діють від імені Організації, а також на всі системи та засоби, що використовуються для обробки персональних даних.

1.3. Обробка персональних даних здійснюється відповідно до чинного законодавства, етичного кодексу Організації та стандартів конфіденційності, підписаних в рамках угод про нерозголошення (NDA), зокрема стандартів ЮНІСЕФ.

1.4. Особлива увага приділяється захисту персональних даних осіб, що належать до категорій з підвищеним ризиком розголошення або чутливих даних, включно з дітьми та іншими вразливими групами.

2. ВИЗНАЧЕННЯ ТА ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Персональні дані – це будь-яка інформація, що дозволяє ідентифікувати фізичну особу, включно з контактними даними, даними про зайнятість, реквізитами документів та іншою конфіденційною інформацією.

2.2. Обробка персональних даних здійснюється на основі принципів: законності та прозорості, мінімізації даних – збір лише тих даних, які необхідні для визначеної мети, точності та актуальності даних, забезпечення безпеки та конфіденційності.

2.2. Організація дотримується принципу мінімізації даних та збирає лише ті персональні дані, які є необхідними для реалізації програмної діяльності, виконання договірних або юридичних зобов’язань чи забезпечення захисту бенефіціарів.

2.4. Збір та використання персональних даних:

2.4.1. Персональні дані збираються лише після отримання чіткого погодження суб’єкта даних (бенефіціара).

2.4.2. Зібрані дані використовуються виключно для цілей реалізації конкретного проєкту або завдання Організації.

2.4.3. Використання персональних даних для інших цілей без нового погодження заборонене.

2.4.4. Всі бенефіціари мають право отримати інформацію про те, які дані збираються, для чого вони будуть використані та як довго зберігатимуться.

2.5. Персональні дані неповнолітніх:

2.5.1. Збір персональних даних осіб віком до 18 років здійснюється лише за письмовим погодженням батьків або законних представників.

2.5.2. Дані неповнолітніх обробляються виключно для цілей конкретного проєкту або завдання Організації.

2.5.3. Доступ до персональних даних неповнолітніх обмежується мінімально необхідним колом відповідальних осіб.
2.5.4. Дані неповнолітніх зберігаються в зашифрованому вигляді та підлягають регулярному резервному копіюванню, з дотриманням правил інформаційної безпеки.
2.5.5. Після завершення цілей проєкту або досягнення строків зберігання дані неповнолітніх видаляються або анонімізуються.
2.6. Правові підстави обробки персональних даних:
2.6.1. Організація здійснює обробку персональних даних на підставі:

- добровільної згоди суб'єкта персональних даних;
- виконання договірних або грантових зобов'язань;
- виконання вимог законодавства України;
- захисту життєво важливих інтересів бенефіціарів або працівників/ць;
- реалізації статутної діяльності Організації.

2.7. Організація може використовувати форми згоди на обробку персональних даних відповідно до Додатку 4 до цієї Політики.

3. ОБОВ'ЯЗКИ ТА ВІДПОВІДАЛЬНІ ОСОБИ

3.1. Відповідальними за реалізацію цієї Політики є:
Головний/а бухгалтер/ка – забезпечує конфіденційність фінансових і кадрових даних, здійснює резервне копіювання баз даних, контролює обмеження доступу до систем обліку;
Офіцер з моніторингу та оцінки – координує виконання політики щодо захисту персональних даних, проводить регулярний моніторинг дотримання правил обробки даних, здійснює оцінку ризиків та надає рекомендації щодо покращення заходів безпеки;
Особи, які представляють та діють від імені Організації – дотримуються правил доступу до персональних даних, забезпечують конфіденційність під час виконання робочих завдань, використовують засоби захисту (паролі, двоетапну верифікацію), дотримуються процедур виходу з систем після роботи на сторонніх пристроях.
3.2. Всі зазначені особи зобов'язані: дотримуватися правил конфіденційності та обробки персональних даних, своєчасно повідомляти про будь-які порушення або загрози безпеці даних, проходити навчання та ознайомлюватися з оновленнями цієї Політики, виконувати додаткові заходи безпеки, передбачені внутрішніми регламентами Організації.
3.3. Доступ до персональних даних надається лише тим працівникам/цям або залученим особам, яким така інформація необхідна для виконання службових або проєктних обов'язків.
3.4. Організація проводить регулярні навчання або інформування працівників/ць щодо захисту персональних даних, конфіденційності та інформаційної безпеки.

4. ЗАХОДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Для запобігання несанкціонованого доступу встановлюються:
паролі на персональні комп'ютери відповідальних осіб, двоетапна верифікація на доступних системах комунікації та обліку, обмежений доступ до інформаційних баз за допомогою систем адміністрування.
4.2. Паролі та ключі доступу є конфіденційною інформацією і не можуть передаватися стороннім особам.
4.3. У разі роботи на сторонніх пристроях працівник зобов'язаний вийти з усіх авторизованих облікових записів після завершення роботи.
4.4. Для категорій підвищеного ризику застосовуються додаткові методи захисту, включно з шифруванням корпоративного рівня та VPN.
4.5. Під час дистанційної роботи працівники/ці та інші залучені особи повинні використовувати захищені пристрої, паролі доступу, уникати використання публічних незахищених мереж Wi-Fi та забезпечувати конфіденційність персональних даних під час роботи поза офісом.

5. ОБРОБКА ТА ЗБЕРІГАННЯ ПЕРСОНАЛЬНИХ ДАНИХ
5.1. Персональні дані зберігаються у захищених інформаційних системах, на сервері та в хмарному сховищі.
5.2. Резервне копіювання баз даних здійснюється щомісяця відповідальними особами.
5.3. Кодування та шифрування персональних даних:
5.3.1. Усі персональні дані, що обробляються в Організації, підлягають кодуванню або шифруванню для запобігання несанкціонованому доступу.
5.3.2. Методи шифрування обираються таким чином, щоб гарантувати конфіденційність даних та їх захист від сторонніх осіб.
5.3.3. Відповідальні за обробку персональних даних особи контролюють: доступ до ключів шифрування, збереження зашифрованих даних у захищених інформаційних системах, на сервері та в хмарному сховищі, резервне копіювання зашифрованих даних.
5.3.4. Будь-яке розкриття ключів шифрування стороннім особам заборонено, крім випадків, передбачених законодавством або внутрішніми регламентами Організації.
5.3.5. Офіцер з моніторингу та оцінки контролює дотримання правил кодування та шифрування та проводить регулярну оцінку ризиків щодо безпеки персональних даних.
5.4. Строки зберігання персональних даних визначаються відповідно до законодавства України, вимог донорів, договірних зобов'язань та внутрішніх процедур Організації. Організація прагне не зберігати персональні дані довше, ніж це необхідно для досягнення цілей їх обробки. Після завершення строків зберігання або досягнення мети обробки персональні дані підлягають видаленню, анонімізації або знищенню відповідно до внутрішніх процедур Організації. Детальні строки зберігання окремих категорій персональних даних можуть визначатися у Додатку 1 до цієї Політики.

5.5. Знищення та утилізація персональних даних:
5.5.1. Документи та носії інформації, що містять персональні дані, підлягають знищенню після завершення строків зберігання або досягнення цілей їх обробки.
5.5.2. Паперові документи з персональними даними утилізуються шляхом подрібнення або іншим способом, що виключає можливість відновлення інформації.
5.5.3. Електронні документи видаляються із систем з використанням засобів, що забезпечують неможливість відновлення даних.
5.5.4. Відповідальність за своєчасне та правильне знищення персональних даних несуть відповідальні особи, зазначені у розділі 3.

6. КОНФІДЕНЦІЙНІСТЬ ТА НЕРОЗГОЛОШЕННЯ

6.1. Усі працівники/ці та представники/ці Організації підписують угоди про нерозголошення (NDA), які включають правила зберігання, обробки та передачі персональних даних.
6.2. Передача персональних даних стороннім особам можлива лише у випадках, передбачених законодавством або внутрішніми регламентами Організації.
6.3. Передача персональних даних партнерам, підрядникам або постачальникам послуг здійснюється відповідно до вимог цієї Політики та принципів, визначених у Додатку 2 до цієї Політики.
6.4. Передача персональних даних партнерам, підрядникам або постачальникам послуг здійснюється лише за умови наявності відповідних гарантій захисту даних та виключно в межах, необхідних для реалізації діяльності Організації.
6.5. Передбачається використання захищених каналів комунікації (шифровані листування, форми збору).

7. ПРАВА СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

7.1. Суб'єкти персональних даних мають право: доступу до власних даних, виправлення, уточнення та оновлення даних, вимоги про видалення або обмеження обробки даних, подання скарг на порушення правил обробки персональних даних.

8. РЕАГУВАННЯ НА ІНЦИДЕНТИ

8.1. Будь-яке порушення безпеки даних фіксується та розслідується;
8.2. При серйозних інцидентах повідомляються грантодавці та відповідні органи;
8.3. Вживаються заходи для запобігання повторенню інциденту.
8.4. Організація прагне повідомляти про суттєві порушення безпеки персональних даних керівництво, відповідальних осіб та, за потреби, донорів або партнерів у максимально короткі строки після виявлення інциденту.
8.5. У разі діяльності, пов'язаної з підвищеним ризиком для персональних даних, Організація може проводити оцінку впливу на захист персональних

даних (Data Protection Impact Assessment - DPIA) відповідно до Додатку 3 до цієї Політики.
8.6. Організація може вести внутрішній журнал інцидентів, пов'язаних із захистом персональних даних, з метою моніторингу, реагування та запобігання повторним порушенням відповідно до Додатку 5 до цієї Політики.

9. КОНТРОЛЬ ТА ВНЕСЕННЯ ЗМІН
9.1. Контроль за виконанням цієї Політики здійснює Офіцер з моніторингу та оцінки.
9.2. Зміни до Політики можуть вноситися за рішенням керівництва Організації та підлягають обов'язковому ознайомленню всіх працівників.

ДОДАТОК 1
Строки зберігання персональних даних

Категорія даних	**Приклад**	**Орієнтовний строк**
Дані працівників/ць	трудові документи, контракти	відповідно до законодавства України
Дані бенефіціарів	реєстраційні форми, списки учасників	до завершення проєкту + до 3 років (якщо інше не вимагається донором)
Дані дітей	форми згоди, форми відвідування	мінімально необхідний строк
Фінансова документація	платежі, договори, звіти	відповідно до вимог законодавства та донорів
Фото/відео матеріали	комунікаційні матеріали	до відкликання згоди або завершення потреби використання
Incident/Breach records	внутрішні розслідування	до 5 років або відповідно до вимог донорів

ДОДАТОК 2
Основні принципи передачі персональних даних третім сторонам

Організація може передавати персональні дані партнерам, підрядникам або постачальникам послуг лише за умови:

- наявності законної підстави для передачі даних;
- дотримання принципу мінімізації даних;
- забезпечення належного рівня захисту персональних даних;
- використання даних виключно для визначених цілей;
- дотримання конфіденційності та вимог safeguarding.

Особи або організації, які отримують доступ до персональних даних, повинні забезпечувати:

- захист персональних даних;
- обмеження доступу до інформації;
- недопущення несанкціонованого поширення даних;
- безпечне зберігання та передачу інформації.

ДОДАТОК 3
Процедура оцінки впливу на захист персональних даних (DPIA)

Організація може проводити оцінку впливу на захист персональних даних у випадках:

- обробки великих обсягів персональних даних;
- роботи з чутливими категоріями даних;
- роботи з даними дітей;
- впровадження нових цифрових систем;
- реалізації діяльності з підвищеним рівнем ризику.

Оцінка впливу може включати:

- опис діяльності з обробки даних;
- визначення потенційних ризиків;
- оцінку можливого впливу на суб’єктів даних;
- визначення заходів мінімізації ризиків;
- визначення відповідальних осіб.

Рішення про необхідність проведення DPIA приймається керівництвом Організації або відповідальною особою з урахуванням характеру діяльності та рівня ризику.

ДОДАТОК 4
Приклад форми згоди на обробку персональних даних

Я, _____, надаю добровільну згоду БЛАГОДІЙНІЙ ОРГАНІЗАЦІЇ «БФ «ДОБРОБУТ УКРАЇНИ» на обробку моїх персональних даних з метою участі у програмній діяльності Організації.
Мені повідомлено про:

- мету збору персональних даних;
- обсяг даних, що обробляються;
- можливу передачу даних партнерам або донорам у межах реалізації проєкту;
- строки зберігання даних;
- мої права як суб'єкта персональних даних.

Дата: _____

Підпис: _____

Для дітей:

Я, _____,
як законний представник дитини _____,
надаю згоду на обробку персональних даних дитини відповідно до мети діяльності Організації.

ДОДАТОК 5
Журнал інцидентів, пов'язаних із захистом персональних даних

Дата	Опис інциденту	Категорія даних	Потенційний ризик	Вжиті заходи	Відповідальна особа

Голова Правління **Вікторія ПРЕОБРАЖЕНСЬКА**

З Політикою ознайомлені:

Офіцер з моніторингу та оцінки
Іоанн ПРЕОБРАЖЕНСЬКИЙ

Дата: «05» серпня 2025 р.