

БЛАГОДІЙНА ОРГАНІЗАЦІЯ
«БЛАГОДІЙНИЙ ФОНД «ПРАВО НА ЗАХИСТ»
(БФ «ПРАВО НА ЗАХИСТ»)

Код ЄДРПОУ 38621206

НАКАЗ

«23» грудня 2025 р.

Київ

№ 216-з

Про затвердження Стандартної операційної процедури
«Захист персональних даних благодійників та користувачів сайту»

З метою упорядкування процесів збору, обробки та захисту персональних даних благодійників і користувачів офіційних онлайн-ресурсів Фонду, забезпечення відповідності діяльності законодавству України та принципам GDPR, а також на виконання Політики конфіденційності та захисту персональних даних, керуючись Статутом Фонду,

НАКАЗУЮ:

1. **Затвердити** Стандартну операційну процедуру «Захист персональних даних благодійників та користувачів сайту» Благодійної організації «Благодійний Фонд «Право на захист» (додається).
2. Співробітникам Фонду неухильно дотримуватись вимог та рекомендацій даної Політики.
3. Контроль за виконанням цього наказу залишаю за собою.

Президент «БФ «ПРАВО НА ЗАХИСТ»



Олександр ГАЛКІН



ЗАТВЕРДЖЕНО
Наказ БФ «Право на Захист»
«23» грудня 2025 р № 216-з

***СТАНДАРТНА ОПЕРАЦІЙНА ПРОЦЕДУРА
ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ БЛАГОДІЙНИКІВ ТА
КОРИСТУВАЧІВ САЙТУ***

БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ
“БЛАГОДІЙНИЙ ФОНД “ПРАВО НА ЗАХИСТ”

ЗМІСТ

I. Мета і завдання.....	3
II. Основні поняття.	3
III. Сфера застосування.	3
IV. Ролі та відповідальність.....	4
V. Категорія персональних даних, що обробляється.	5
VI. Мета обробки персональних даних.	5
VII. Порядок отримання згоди.	6
VIII. Особливості обробки платіжних даних та використання файлів cookie.....	6
IX. Передача даних третім сторонам.	7
X. Права благодійників та користувачів сайту та строки зберігання даних.....	7
XI. Безпека та інциденти.	8

I. МЕТА І ЗАВДАННЯ

1.1. Стандартна операційна процедура Захисту персональних даних благодійників та користувачів сайту (далі – **Процедура**) визначає порядок збору, обробки, зберігання та захисту персональних даних:

- благодійників (фізичних та юридичних осіб);
- користувачів офіційного веб-сайту Фонду та інших онлайн ресурсів, що адмініструються Фондом.

1.2. Мета Процедури:

- забезпечити прозорий та безпечний обіг персональних даних;
- виконати вимоги законодавства України у сфері захисту персональних даних та принципи GDPR;
- захистити права благодійників і користувачів сайту на приватність та контроль над своїми даними.

II. ОСНОВНІ ПОНЯТТЯ.

2.1. **Благодійник** – фізична або юридична особа, яка добровільно надає Фонду кошти, майно чи іншу підтримку для реалізації статутної діяльності та благодійних програм.

2.2. **Донор** – міжнародна, державна, приватна або корпоративна установа, фонд чи організація, яка надає фінансову, технічну або експертну підтримку Фонду.

2.3. **Користувач сайту** – будь-яка особа, яка відвідує офіційний веб-сайт Фонду або інші онлайн ресурси Фонду.

2.4. **Файли cookie** – невеликі текстові файли, які зберігаються на пристрої користувача (комп'ютер, планшет, телефон) під час відвідування веб-сайту. Вони використовуються для забезпечення стабільної роботи сайту, запам'ятовування налаштувань, спрощення навігації та збору узагальненої статистики. Cookie не ідентифікують користувача особисто.

2.5. **Офіційний веб-сайт Фонду** – веб-сайт, який адмініструється Фондом, та інші онлайн ресурси, прямо зазначені на ньому як офіційні.

III. СФЕРА ЗАСТОСУВАННЯ.

3.1. Процедура поширюється на всіх працівників Фонду, залучених спеціалістів, підрядників та інших осіб, які:

- мають доступ до персональних даних благодійників;
- мають доступ до даних користувачів офіційного веб-сайту Фонду та інших онлайн ресурсів;
- беруть участь в організації та адмініструванні збору благодійних внесків (онлайн та офлайн).

3.2. Процедура застосовується до всіх офіційних онлайн ресурсів Фонду:

- офіційний веб-сайт Фонду;
- сторінки у соціальних мережах;
- платформи для збору пожертв (наприклад, Monobank, GlobalGiving, інші сервіси);
- форми зворотного зв'язку, підписки на розсилки, реєстраційні форми тощо.

IV. РОЛІ ТА ВІДПОВІДАЛЬНІСТЬ.

4.1. Керівник відділу фандрейзингу та партнерств:

- відповідає за дотримання цієї Процедури в частині, що стосується роботи з персональними даними благодійників і донорів у межах фандрейзингових процесів;
- забезпечує належне інформування благодійників про умови обробки їхніх даних;
- контролює, щоб персональні дані благодійників використовувалися працівниками відділу **лише для дозволених цілей** (комунікація, розсилки, підтвердження внесків);
- передає уповноваженій особі з питань захисту даних **пропозиції щодо оновлення** цієї Процедури, якщо змінюються фандрейзингові інструменти або канали взаємодії.

4.2. IT/технічний спеціаліст (або підрядник):

- забезпечує технічний захист даних (SSL/HTTPS, захищені сервери, резервне копіювання);
- налаштовує та підтримує роботу форм збору даних на веб-сайті, cookie та інших технічних елементів, необхідних для їх коректного функціонування та безпеки;
- забезпечує надання, зміну та відкликання технічних доступів працівникам відповідно до принципу “необхідності знання”.

4.3. Фінансовий відділ / бухгалтерія:

- використовує дані благодійників виключно для цілей обліку, звітності та підтвердження платежів;
- не обробляє та не зберігає реквізити платіжних карток (номери карток, CVV тощо), оскільки такі дані не надходять до Фонду від платіжних сервісів;
- забезпечує належне зберігання фінансових даних відповідно до законодавчих вимог та внутрішніх процедур.

4.4. Усі працівники, які працюють з даними благодійників та користувачів сайту:

- зобов’язані дотримуватись цієї Процедури та Політики конфіденційності та захисту персональних даних Фонду;
- використовують персональні дані лише в межах своїх посадових обов’язків;
- не передають персональні дані третім сторонам без законних підстав або згоди особи;
- зобов’язані **негайно повідомляти уповноважену особу або свого керівника** про будь-яку підозру порушення безпеки персональних даних.

4.5. Уповноважена особа з питань захисту персональних даних (або визначений наказом працівник) відповідає за:

- розглядає запити суб’єктів персональних даних та забезпечує своєчасну відповідь відповідно до законодавства;
- координує виконання цієї Процедури та контролює відповідність вимогам законодавства та Політики Фонду;
- перевіряє правильність фіксації згод та дотримання строків зберігання персональних даних у відповідних системах;
- веде облік та документує інциденти, пов’язані з порушеннями безпеки персональних даних, і координує заходи реагування;
- реагує на інциденти витоку персональних даних відповідно до Плану реагування.

V. КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ.

5.1. Фонд може обробляти персональні дані фізичних осіб, які роблять благодійні внески або взаємодіють з Фондом через онлайн чи офлайн канали. До таких даних можуть належати:

- ідентифікаційні дані: ім'я, прізвище, по батькові, ПІН (РНОКПП);
- контактні дані: електронна адреса, номер телефону;
- локалізаційні дані: країна або місто проживання (якщо вказано);
- платіжна інформація: сума, дата, валюта та спосіб здійснення внеску (без реквізитів картки);
- комунікаційні налаштування: підписка на розсилки, згода на отримання інформаційних повідомлень.

5.2. Для юридичних осіб, компаній-партнерів та організацій, що надають благодійну підтримку, можуть оброблятися такі категорії даних:

- ідентифікаційні дані організації: назва компанії або установи;
- реєстраційні дані: код ЄДРПОУ або інший юридичний ідентифікатор;
- контактна інформація відповідальної особи: ПІБ, посада, телефон, електронна адреса;
- фінансові та платіжні реквізити (у межах, необхідних для бухгалтерського обліку й звітності);
- дані про взаємодію: інформація про здійснені внески, укладені договори, звітність.

5.3. Під час відвідування сайту або взаємодії з іншими онлайн ресурсами Фонду можуть оброблятися такі дані:

- **дані, які користувач надає свідомо:** ім'я, електронна адреса, номер телефону (наприклад, через форми зворотного зв'язку, підписки, реєстрації);
- **технічні знеособлені дані:** IP-адреса, тип браузера, операційна система, мова, тип пристрою, час взаємодії з сайтом;
- **дані cookie:** налаштування мови, параметри сеансу, інформація про переглянуті сторінки та інші технічні показники, необхідні для роботи сайту та аналітики.

VI. МЕТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ.

6.1. Персональні дані благодійників та користувачів онлайн ресурсів обробляються Фондом виключно для забезпечення ефективної, безпечної та прозорої діяльності. Основні цілі такі:

6.1.1. Проведення благодійних платежів та обліку внесків. Фонд обробляє дані, щоб забезпечити можливість здійснення внесків онлайн та офлайн, правильно зафіксувати кожен платіж, підтвердити його отримання та коректно відобразити у фінансових системах.

6.1.2. Фінансовий облік і звітність. Дані використовуються для ведення бухгалтерського обліку, формування фінансової та податкової звітності, а також для виконання вимог донорів, партнерів і державних органів.

6.1.3. Комунікація та підтримка взаємодії з благодійниками. Фонд використовує контактні дані благодійників для:

- надсилання підтверджень про отримання внесків;
- інформування про те, як були використані кошти та яких результатів досягнуто;
- розсилки новин, запрошень та повідомлень — **лише за наявності згоди благодійника.**

Це дозволяє будувати довіру та підтримувати відкритий діалог із тими, хто підтримує діяльність Фонду.

6.1.4. Забезпечення прозорості та підзвітності діяльності Фонду. Фонд обробляє дані, щоб гарантувати прозорість використання благодійних внесків, дотримання законодавства та стандартів доброчесності. Це включає аудит, внутрішній контроль та підготовку публічних звітів.

6.1.5. Забезпечення стабільної та безпечної роботи веб-сайту та інших онлайн ресурсів. Під час відвідування сайту можуть оброблятися технічні дані, необхідні для:

- аналізу статистики відвідувань і покращення роботи сайту.

6.2. Персональні дані благодійників та користувачів онлайн ресурсів обробляються на підставах, визначених законодавством України та GDPR, зокрема:

- на підставі згоди суб'єкта персональних даних;
- для виконання договору або вчинення дій, необхідних перед укладенням договору;
- для виконання юридичних обов'язків Фонду;
- на підставі легітимного інтересу Фонду (забезпечення безпеки ресурсів, запобігання шахрайству, ведення внутрішньої аналітики тощо).

VII. ПОРЯДОК ОТРИМАННЯ ЗГОДИ.

7.1. Благодійник або користувач сайту надає згоду на обробку персональних даних шляхом вчинення однієї або кількох дій:

- під час здійснення благодійного внеску через веб-сайт – шляхом проставлення позначки (чекбокс) про згоду з Політикою конфіденційності та захисту персональних даних та натискання кнопки «Підтвердити платіж», «Підтримати» тощо;
- під час заповнення онлайн форм (заявки на участь, підписка на розсилку, форма зворотного зв'язку) – шляхом заповнення полів і відправлення форми;
- під час укладення договору або підписання інших документів офлайн;
- під час комунікації електронною поштою або в соціальних мережах, якщо особа добровільно надає свої контактні дані.

7.2. Надання персональних даних означає згоду особи на їх обробку Фондом відповідно до Політики конфіденційності та захисту персональних даних та цієї Процедури.

7.3. Благодійник/користувач може у будь-який момент відкликати свою згоду, надіславши запит на офіційну адресу Фонду privacy@r2p.org.ua.

VIII. ОСОБЛИВОСТІ ОБРОБКИ ПЛАТІЖНИХ ДАНИХ ТА ВИКОРИСТАННЯ ФАЙЛІВ СООКІЕ.

8.1. Фонд не зберігає та не обробляє реквізити платіжних карток (номери карток, строк дії, CVV тощо).

8.2. Усі транзакції проводяться через сертифікованих платіжних операторів, які відповідають вимогам безпеки (стандарти на кшталт PCI DSS).

8.3. Фонд отримує від платіжних систем лише інформацію про факт успішного платежу (сума, час, валюта, спосіб оплати, ідентифікатор транзакції) і використовує її для:

- підтвердження внеску;
- ведення фінансового обліку;
- формування звітності.

8.4. Сайт Фонду використовує файли cookie для:

- забезпечення коректної та стабільної роботи сайту;
- запам'ятовування налаштувань користувача (наприклад, мови);
- збору узагальненої статистики про відвідування сайту.

8.5. Деякі cookie можуть дозволяти ідентифікацію пристрою або користувача, якщо це необхідно для роботи веб-сайту чи забезпечення безпеки. Фонд використовує лише ті cookie, які є необхідними або на які користувач надав згоду (якщо застосовно).

8.6. Користувач може самостійно керувати cookie у налаштуваннях браузера (видаляти, блокувати, обмежувати).

ІХ. ПЕРЕДАЧА ДАНИХ ТРЕТІМ СТОРОНАМ.

9.1. Персональні дані благодійників і користувачів сайту можуть передаватися третім сторонам лише у таких випадках:

- для проведення платіжних операцій уповноваженими платіжними операторами;
- для виконання вимог законодавства (на вимогу державних органів у межах їх повноважень);
- за окремою, чітко вираженою згодою благодійника/користувача.

9.2. Усі партнери, яким можуть передаватися дані, зобов'язані дотримуватися конфіденційності та забезпечувати належний рівень захисту даних.

Х. ПРАВА БЛАГОДІЙНИКІВ ТА КОРИСТУВАЧІВ САЙТУ ТА СТРОКИ ЗБЕРІГАННЯ ДАНИХ.

10.1. Благодійник/користувач має право:

- отримати інформацію про те, які його дані обробляє Фонд;
- отримати копію своїх персональних даних;
- вимагати виправлення неточних або застарілих даних;
- вимагати видалення даних у випадках, передбачених законодавством;
- відкликати згоду на обробку даних;
- отримати інформацію про передачу даних третім сторонам;
- подати звернення або скаргу до Фонду чи до Уповноваженого Верховної Ради України з прав людини.

10.2. Персональні дані благодійників зберігаються протягом строку, необхідного для досягнення мети, з якою вони були зібрані, але не довше ніж встановлено внутрішніми документами Фонду (наприклад, не більше 3 років після останнього контакту, якщо законодавство не вимагає більшого строку).

10.3. Імена та інші ідентифікаційні дані благодійників можуть бути опубліковані на сайті Фонду, у звітах чи інших публічних матеріалах лише за наявності окремої згоди благодійника.

10.4. За замовчуванням інформація про внески публікується у знеособленому або агрегованому вигляді.

10.5. Після закінчення строку зберігання дані:

- видаляються або
- знеособлюються (анонімізуються) таким чином, щоб більше не можна було ідентифікувати особу.

XI. БЕЗПЕКА ТА ІНЦИДЕНТИ.

11.1. Фонд застосовує технічні та організаційні заходи для захисту даних:

- шифрування передачі даних (SSL/HTTPS);
- зберігання інформації на захищених серверах;
- системи резервного копіювання;
- обмеження доступу до баз даних (доступ лише для уповноважених осіб);
- регулярний перегляд прав доступу.

11.2. У разі підозри на витік чи несанкціонований доступ до даних діє [План реагування на витік даних](#)