

**БЛАГОДІЙНА ОРГАНІЗАЦІЯ
«БЛАГОДІЙНИЙ ФОНД «САПОРТ ХЕРСОН»**

*Юридична адреса: 03035, м. Київ, провулок Ярослава Хомова, буд. 14 А.
Код ЄДРПОУ 44834913*

НАКАЗ

«10» 10 2023р.

м. Київ

№ 4

**Про затвердження Політики конфіденційності
та захисту персональних даних
Благодійної організації «Благодійний фонд
«Сапорт Херсон»**

Відповідно до статуту Благодійної організації «Благодійний фонд
«Сапорт Херсон»

НАКАЗУЮ:

1. Затвердити Політику конфіденційності та захисту персональних даних Благодійної організації «Благодійний фонд «Сапорт Херсон»
2. Призначити відповідальною особою голову фонду Нісара Ахмада
3. Голові фонду ознайомити працівників фонду з усіма положеннями
4. Контроль за виконанням наказу залишаю за головою фонду

Голова Благодійної організації
«Благодійний фонд «САПОРТ ХЕРСОН»



Нісар АХМАД



БЛАГОДІЙНА ОРГАНІЗАЦІЯ
«БЛАГОДІЙНИЙ ФОНД «САПОРТ ХЕРСОН»
Юридична адреса: 03035, м. Київ, провулок Ярослава Хомова, буд. 14 А.
Код ЄДРПОУ 44834913, e-mail: sup.kherson22@gmail.com

CHARITABLE ORGANIZATION
«CHARITABLE FOUNDATION «SUPPORT KHERSON»
Legal address: Yaroslav Khomov lane, 14 A, Kyiv, 03035
Code 44834913, e-mail: sup.kherson22@gmail.com

Політика конфіденційності та захисту персональних даних Благодійної організації «Благодійний фонд «Сапорт Херсон»

Загальні відомості про документ	
Версія документа	Версія 1
Перелік посад (осіб), кого стосується цей документ	Працівники та волонтери БО «БФ «Сапорт Херсон» та бенефіціари
Документ затверджено (посада, ПІБ)	Голова БО «БФ «Сапорт Херсон» Нісар Ахмад
Дата затвердження документу	10.10.2023
Період перегляду документу	за необхідністю, згідно вимог законодавства

Голова Благодійної організації
«Благодійний фонд «САПОРТ ХЕРСОН»



Нісар АХМАД

ЗМІСТ

1. Загальні положення	
1.1. Мета та сфера застосування.....	2
1.2. Ключові терміни.....	2
1.3. Нормативна база.....	2
2. Принципи обробки персональних даних.....	3
2.1. Законність, справедливість та прозорість.....	3
2.2. Обмеження метою та мінімізація даних.....	3
2.3. Точність та обмеження зберігання.....	3
2.4. Цілісність та конфіденційність.....	3
3. Правові підстави обробки, ролі та відповідальність.....	4
3.1. Правові підстави обробки даних.....	4
3.2. Ролі та відповідальність у Фонді.....	4
3.3. Бази персональних даних.....	4
4. Права суб'єктів персональних даних.....	5
4.1. Право на доступ та інформацію.....	5
4.2. Право на виправлення та видалення.....	5
4.3. Право на обмеження обробки та заперечення.....	5
4.4. Порядок реалізації прав.....	5
5. Заходи безпеки та конфіденційність	6
5.1. Організаційні заходи безпеки.....	6
5.2. Технічні заходи безпеки.....	6
5.3. Передача даних третім особам.....	6
6. Реагування на витоки даних.....	7
6.1. Порядок дій при інциденті.....	7
6.2. Інформування наглядових органів та суб'єктів даних.....	7
7. Прикінцеві положення.....	8
7.1. Порядок перегляду Політики.....	8
7.2. Відповідальність за порушення.....	8
Додаток 1. Форма згоди на обробку персональних даних.....	9

Розділ 1. Загальні положення

1.1. Мета та сфера застосування Ця Політика встановлює єдині принципи, правила та процедури щодо збору, обробки, зберігання та захисту персональних даних бенефіціарів, співробітників, волонтерів та партнерів Благодійного фонду «Сапорт Херсон» (далі – Фонд). Метою є забезпечення відповідності діяльності Фонду вимогам Закону України «Про захист персональних даних» та ключовим принципам Загального регламенту про захист даних (GDPR), а також гарантування захисту прав та свобод фізичних осіб. Політика є обов'язковою для всіх співробітників, волонтерів, підрядників та інших осіб, які діють від імені Фонду та мають доступ до персональних даних.

1.2. Ключові терміни

- **Персональні дані:** Будь-яка інформація, що дозволяє прямо чи опосередковано ідентифікувати фізичну особу (суб'єкта даних), така як ім'я, прізвище, контактні дані, ідентифікаційний номер, дані про місцезнаходження тощо.
- **Суб'єкт даних:** Фізична особа, якої стосуються персональні дані та яка може бути ідентифікована за цими даними (бенефіціар, співробітник, волонтер).
- **Обробка даних:** Будь-яка дія або сукупність дій з персональними даними, включаючи збір, запис, організацію, зберігання, використання, передачу, знеособлення та знищення.
- **Володілець даних:** Благодійний фонд «Сапорт Херсон», який визначає мету та засоби обробки персональних даних.
- **Згода суб'єкта даних:** Будь-яке добровільне, конкретне, інформоване та однозначне волевиявлення, у формі заяви або чіткої ствердної дії, яким суб'єкт даних погоджується на обробку своїх персональних даних.

1.3. Нормативна база Ця Політика розроблена на основі та з дотриманням:

- Закону України «Про захист персональних даних» № 2297-VI від 01.06.2010.
- Основних принципів та підходів Загального регламенту про захист даних (ЄС) 2016/679 (GDPR).
- Статуту та інших внутрішніх положень Фонду.

Розділ 2. Принципи обробки персональних даних

Фонд зобов'язується дотримуватися наступних фундаментальних принципів при будь-якій обробці персональних даних для забезпечення найвищого рівня захисту та поваги до прав людини.

2.1. Законність, справедливість та прозорість Персональні дані обробляються на законних підставах, справедливо та у прозорий спосіб для суб'єкта даних. Фонд завжди інформує осіб про те, які дані, з якою метою та в який спосіб збираються та обробляються.

2.2. Обмеження метою та мінімізація даних Персональні дані збираються лише для чітко визначених, законних та заздалегідь відомих цілей. Фонд забезпечує, що обсяг даних, які обробляються, є адекватним, релевантним та обмежується тим мінімумом, який є необхідним для досягнення заявленої мети.

2.3. Точність та обмеження зберігання Фонд вживає всіх розумних заходів для забезпечення точності та актуальності персональних даних. Дані, що є неточними, виправляються або видаляються без зволікань. Персональні дані зберігаються у формі, що дозволяє ідентифікацію суб'єкта, не довше, ніж це необхідно для цілей, з якими ці дані оброблялися.

2.4. Цілісність та конфіденційність Фонд забезпечує належний рівень безпеки персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення чи пошкодження, шляхом впровадження відповідних технічних та організаційних заходів.

Розділ 3. Правові підстави обробки, ролі та відповідальність

3.1. Правові підстави обробки даних

Фонд здійснює обробку персональних даних виключно за наявності однієї з наступних законних підстав:

- **Згода:** Обробка здійснюється на підставі добровільної, інформованої та однозначної згоди суб'єкта даних на обробку його персональних даних для однієї або кількох конкретних цілей. Форма для отримання згоди наведена у Додатку 1.
- **Виконання договору:** Обробка є необхідною для укладення або виконання договору, стороною якого є суб'єкт даних (наприклад, трудові договори зі співробітниками, договори з підрядниками).
- **Законний інтерес:** Обробка є необхідною для цілей законних інтересів Фонду (наприклад, для проведення моніторингу та оцінки програм, внутрішньої аналітики, забезпечення безпеки), за винятком випадків, коли інтереси або основні права та свободи суб'єкта даних переважають такі інтереси.

3.2. Ролі та відповідальність у Фонді

- **Голова Фонду:** Несе загальну відповідальність за забезпечення відповідності діяльності Фонду законодавству про захист персональних даних.
- **Відповідальна особа за захист даних:** Призначається наказом Голови Фонду. Ця особа є центральною контактною точкою з питань захисту даних, відповідає за моніторинг дотримання цієї Політики, консультування персоналу та розгляд запитів від суб'єктів даних.
- **Керівники відділів:** Забезпечують дотримання цієї Політики співробітниками у своїх підрозділах та контролюють доступ до персональних даних.
- **Усі співробітники та волонтери:** Несуть персональну відповідальність за дотримання правил конфіденційності та безпеки при роботі з персональними даними, до яких вони мають доступ.

3.3. Бази персональних даних

Фонд є володільцем наступних основних баз персональних даних:

- **База даних бенефіціарів:** Створюється з метою надання гуманітарної допомоги, моніторингу, оцінки та звітності. Містить дані, необхідні для ідентифікації отримувачів допомоги, оцінки їхніх потреб та верифікації наданих послуг.
- **База даних персоналу та волонтерів:** Створюється з метою ведення кадрового діловодства, нарахування заробітної плати, виконання вимог законодавства та управління діяльністю команди.

Розділ 4. Права суб'єктів персональних даних

Фонд гарантує та забезпечує дотримання всіх прав суб'єктів даних, передбачених законодавством. Кожна особа, чії персональні дані обробляються Фондом, має наступні права:

4.1. Право на доступ та інформацію Суб'єкт даних має право отримати від Фонду підтвердження, чи обробляються його персональні дані, а також отримати доступ до цих даних та вичерпну інформацію щодо мети обробки, категорій даних, отримувачів та термінів зберігання.

4.2. Право на виправлення та видалення ("право бути забутим") Суб'єкт даних має право вимагати негайного виправлення неточних персональних даних, що його стосуються. Також він має право вимагати видалення своїх даних, якщо вони більше не є потрібними для цілей, для яких їх було зібрано, або якщо було відкликано згоду на їх обробку.

4.3. Право на обмеження обробки та заперечення Суб'єкт даних має право вимагати обмеження обробки своїх даних у певних випадках (наприклад, на час перевірки їх точності). Також він має право в будь-який момент заперечити проти обробки своїх даних, якщо вона здійснюється на підставі законного інтересу Фонду.

4.4. Порядок реалізації прав

- Для реалізації своїх прав суб'єкт даних повинен подати письмовий запит (електронним або звичайним листом) на ім'я **Відповідальної особи за захист даних** Фонду.
- Фонд може попросити надати додаткову інформацію для ідентифікації особи заявника, щоб запобігти несанкціонованому доступу до даних.
- Фонд зобов'язується надати відповідь на запит без невиправданої затримки, але не пізніше **одного місяця** з моменту отримання запиту.
- Реалізація прав суб'єкта даних здійснюється на безоплатній основі.

Розділ 5. Заходи безпеки та конфіденційність

Фонд вживає комплексних організаційних та технічних заходів для забезпечення належного рівня захисту персональних даних від несанкціонованого доступу, зміни, розкриття або знищення.

5.1. Організаційні заходи безпеки

- **Принцип обмеженого доступу:** Доступ до персональних даних надається співробітникам та волонтерам суворо на основі їхніх посадових обов'язків ("need-to-know basis").
- **Навчання персоналу:** Фонд проводить регулярні обов'язкові тренінги для всього персоналу з питань політик та процедур захисту даних.
- **Договори про нерозголошення:** Усі співробітники, волонтери та підрядники, які мають доступ до конфіденційної інформації, підписують зобов'язання про нерозголошення.
- **Фізична безпека:** Паперові документи, що містять чутливі персональні дані, зберігаються у шафах або приміщеннях, що замикаються, з обмеженим доступом.

5.2. Технічні заходи безпеки

- **Контроль доступу:** Доступ до електронних баз даних та систем захищений унікальними логінами та паролями. Для критично важливих систем застосовується двофакторна автентифікація.
- **Шифрування:** Чутливі персональні дані, що зберігаються на портативних пристроях (ноутбуках, зовнішніх дисках) або передаються через незахищені мережі, підлягають шифруванню.
- **Захист від шкідливого ПЗ:** Усі комп'ютери та сервери Фонду оснащені ліцензійним антивірусним програмним забезпеченням, яке регулярно оновлюється.
- **Безпечне знищення даних:** Електронні та паперові носії, що містять персональні дані і термін зберігання яких сплив, знищуються у спосіб, що унеможлиблює їх відновлення (шредування, безпечне стирання даних).

5.3. Передача даних третім особам

Фонд не передає персональні дані третім особам, за винятком наступних випадків:

- Отримано пряму та інформовану згоду від суб'єкта даних.
- Передача вимагається законодавством України (наприклад, на запит державних органів).
- Передача необхідна для звітування перед донором згідно з умовами грантової угоди. У таких випадках Фонд докладає зусиль для передачі даних у знеособленому або агрегованому вигляді.
- Передача здійснюється партнеру по імплементації для надання допомоги бенефіціару, що регулюється договором із суворими положеннями про конфіденційність.

Розділ 6. Реагування на витоки даних

6.1. Порядок дій при інциденті

- **Негайне повідомлення:** Будь-який співробітник або волонтер, який виявив або підозрює інцидент, пов'язаний з порушенням безпеки персональних даних (витік, втрата, несанкціонований доступ), зобов'язаний **негайно** повідомити про це свого безпосереднього керівника та **Відповідальну особу за захист даних**.
- **Первинна оцінка:** Відповідальна особа за захист даних проводить негайну первинну оцінку інциденту для визначення характеру порушення, категорій та кількості зачеплених суб'єктів даних, а також потенційних ризиків.
- **Стимування інциденту:** Вживаються негайні заходи для припинення порушення та мінімізації його наслідків (наприклад, ізоляція ураженої системи, зміна паролів доступу).

6.2. Інформування наглядових органів та суб'єктів даних

- **Інформування наглядового органу:** Якщо витік даних може становити ризик для прав та свобод фізичних осіб, Фонд без невинуватої затримки, і, за можливості, **не пізніше 72 годин** з моменту, коли стало відомо про інцидент, повідомляє про нього уповноважений наглядовий орган з питань захисту персональних даних.
- **Інформування суб'єктів даних:** Якщо встановлено, що витік даних може створити **високий ризик** для прав та свобод фізичних осіб (наприклад, ризик шахрайства, крадіжки особистих даних), Фонд без невинуватої затримки інформує про інцидент безпосередньо зачеплених суб'єктів даних. Повідомлення містить опис характеру інциденту, можливих наслідків та заходів, яких було вжито.

Розділ 7. Прикінцеві положення

7.1. Порядок перегляду Політики

- Ця Політика підлягає обов'язковому перегляду та, за необхідності, оновленню **щонайменше раз на рік**.
- Позачерговий перегляд може бути ініційований у разі суттєвих змін у діяльності Фонду, законодавстві України або вимогах ключових донорів.
- Відповідальність за ініціювання перегляду покладається на Відповідальну особу за захист даних. Зміни до Політики затверджуються наказом Голови Фонду.

7.2. Відповідальність за порушення

- Недотримання положень цієї Політики розглядається як серйозне порушення.
- Будь-який співробітник або волонтер, який порушив цю Політику, може бути притягнутий до дисциплінарної відповідальності згідно з внутрішніми правилами Фонду та чинним законодавством України, що може включати догану або звільнення.

Додаток 1. Форма згоди на обробку персональних даних

Володілець даних: Благодійна організація «Благодійний фонд «Сапорт Херсон» (далі – Фонд).

1. Мета обробки персональних даних Я розумію та погоджуюся, що мої персональні дані (та/або дані дитини, законним представником якої я є) збираються та обробляються Фондом з наступною метою (відмітити необхідне):

- Реєстрація для надання гуманітарної або іншої благодійної допомоги.
- Проведення моніторингу та оцінки якості наданої допомоги.
- Підготовка неперсоніфікованої (анонімної) статистичної звітності для донорів та партнерів.
- Інформування мене про майбутні програми та заходи Фонду.
- Використання фото- та відеоматеріалів з моєю участю (або участю моєї дитини) в комунікаційних та звітних матеріалах Фонду (вебсайт, соціальні мережі, публічні звіти).

2. Обсяг персональних даних, що обробляються Я надаю згоду на обробку наступних категорій моїх персональних даних (та/або даних моєї дитини):

- Прізвище, ім'я, по батькові.
- Контактні дані (номер телефону, адреса електронної пошти).
- Адреса проживання/перебування.
- Дата народження, вік, стать.
- Дані про склад домогосподарства.
- Інформація про статус вразливості (напр., ВПО, особа з інвалідністю, член багатодітної родини).
- Фото- та відеозображення.

3. Ваші права як суб'єкта персональних даних Мене поінформували, що відповідно до Закону України «Про захист персональних даних» я маю право:

- знати про джерела збору, місцезнаходження своїх персональних даних та мету їх обробки;
- отримувати доступ до своїх персональних даних;
- вимагати виправлення неточних даних або їх видалення;
- відкликати свою згоду на обробку персональних даних у будь-який час.

4. Підтвердження згоди

Я, _____ (Прізвище, Ім'я, По батькові повністю), цим підтверджую, що я уважно прочитав(ла) та зрозумів(ла) умови обробки моїх персональних даних, ознайомлений(а) зі своїми правами, і **добровільно надаю свою згоду** БО БФ «Сапорт Херсон» на обробку моїх персональних даних для цілей, зазначених у пункті 1 цієї форми.

Дата: «__» _____ 202_ р.

Підпис: _____