БЛАГОДІЙНА ОРГАНІЗАЦІЯ
«Благодійний фонд «Позитивні Жінки Одеса»
Код ЄДРПОУ: 44866149 м. Одеса, вул. Героїв Оборони Одеси, 56, кв. 37Б

ПОГОДЖЕНО

Протокол засідання Наглядової ради БО «БФ «Позитивні жінки Одеса» № 3 від «29» травня 2026 р.

ЗАТВЕРДЖУЮ

Директорка БО «БФ «Позитивні жінки Одеса»

_____ Гринюк Л.В.

«29» травня 2026 р.

ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

БО «БФ «Позитивні жінки Одеса»

ОДЕСА, 2026

РОЗДІЛ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Цю Політику конфіденційності та захисту персональних даних (далі - Політика) розроблено на виконання вимог Закону України «Про захист персональних даних» та Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» від 03.07.2013 № 383-VII.

1.2. БО «БФ « Позитивні жінки Одеса» захищає права людей, які належать до найвищого ризику щодо інфікування ВІЛ, **(жінки, які живуть з ВІЛ(PLHIV), секс-працівниці (SW), внутрішньо переміщені особи (IDPs), споживачки наркотиків (PWUD), ЛГБТК+, жінки з інвалідністю, люди похилого віку, жінки та дівчата які постраждали від ГЗН, жінки та дівчата які опинилися у скрутному стані)** (далі — бенефіціари).

1.3. Ця Політика встановлює вимоги та процедури збору, обробки та захисту персональних даних бенефіціарів, а також збереження інформації, захисту інформації на публічних ресурсах БО «БФ « Позитивні жінки Одеса» (далі — Організація).

1.4. Організація прагне забезпечити благополуччя бенефіціарів та запобігти шкоди, зловживанням або експлуатації незалежно від віку, здібностей або інвалідності, гендерної ідентичності, раси, релігії, переконань, статі або сексуальної орієнтації, соціально-економічного стану. Організація усвідомлює вразливість багатьох бенефіціарів, особливо жінок та дітей, і бере на себе відповідальність за вжиття розумних та належних заходів для забезпечення їх добробуту в межах діяльності організації.

1.5. З метою реалізації своєї місії та візії Організації зобов'язується просувати Політику у своїй діяльності.

1.6. Метою Політики є:

- забезпечення відповідності діяльності Організації законодавству України та вимогам Загального регламенту про захист персональних даних (GDPR) щодо збору, обробки та зберігання персональних даних бенефіціарів та членів Команди Організації.
- забезпечення механізмами та процедурами захисту та конфіденційності збору, обробки та зберігання персональних даних та інформації про бенефіціарів та членів Команди Організації, а також підвищення рівня свідомості та відповідальності членів Команди Організації у сфері інформаційної безпеки.

1.7. Політика поширюється на всю команду Організації, включно з працівниками, волонтерами, всіма підрядниками, замовниками, партнерськими організаціями, що співпрацюють з Організацією у процесі

реалізації проєктів чи організаційної діяльності, та інші сторони, які є учасниками фінансових чи інших відносин із Організацією.

РОЗДІЛ 2. ОСНОВНІ ПОНЯТТЯ

2.1. *Персональні дані* - будь-яка інформація, що стосується ідентифікованої фізичної особи («бенефіціар», «Член Команди Організації»).

2.2. *Команда Організації* - особи, залучені до реалізації проектів та програм Організації, в тому числі працівники, тимчасово залучені особи, виконавці за цивільно-правовими договорами тощо.

2.3. *Бенефіціар* - це особа, яка безпосередньо отримує товари або послуги в межах програм та проєктів Організації. До осіб, визначених цим терміном, відносяться жінки, які живуть з ВІЛ (PLHIV), секс-працівниці (SW), внутрішньо переміщені особи (IDPs), споживачки наркотиків (PWUD), ЛГБТК+, жінки з інвалідністю, люди похилого віку, жінки та дівчата які постраждали від ГЗН, жінки та дівчата які опинилися у скрутному стані.

2.4. *ВІЛ* – вірус імунодефіциту людини, що зумовлює захворювання на ВІЛ-інфекцію.

2.5. *Вразливі групи населення* – особи або сім'ї, які мають найвищий ризик потрапляння в складні життєві обставини через вплив несприятливих зовнішніх та / або внутрішніх чинників.

2.6. *Обробка персональних даних* – будь-яка операція або сукупність операцій, здійснених з персональними даними, включаючи збір, запис, організацію, збереження, адаптацію, зміну, витяг, консультування, використання, передачу, поширення, об'єднання, блокування, видалення або знищення, тощо.

2.7. *База персональних даних* – організована структура, що містить персональні дані бенефіціарів та забезпечує їх систематизацію та доступ до них.

2.8. *Власник бази персональних даних* – Організація, яка володіє та керує базою персональних даних бенефіціарів та членів Команди Організації визначеною у цій Політиці.

2.9. *Суб'єкт персональних даних* – фізична особа, до якої належать персональні дані та, яка ідентифікована або може бути ідентифікована за допомогою таких даних.

2.10. *Згода суб'єкта персональних даних* – будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки.

2.11. *Знеособлення персональних даних* – вилучення відомостей, які дають змогу ідентифікувати особу.

2.12. *Зберігання інформації* – забезпечення належного стану інформації та її матеріальних носіїв.

2.13. *Конфіденційність інформації* – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

РОЗДІЛ 3. ПРИНЦИПИ ПОВОДЖЕННЯ З ПЕРСОНАЛЬНИМИ ДАНИМИ

3.1. У своїй діяльності Організація дотримується законодавства України та вимог GDPR. Діяльність Організації, яка регулюється вищевказаними нормами, здійснюється за такими принципами:

- *Законність, чесність і прозорість.* Обробка персональних даних здійснюється відкрито та прозоро із застосуванням засобів, що відповідають визначеним цілям такої обробки. У разі зміни визначеної мети обробки персональних даних на нову мету розпорядник персональних даних повинен отримати згоду Суб'єкта персональних даних, якщо інше не передбачено законом.
- *Точність.* Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, що визначається метою їхньої обробки.
- *Обмеження зберігання.* Персональні дані обробляються в допустимій формі, не довше, ніж це необхідно для законних цілей, для яких вони збиралися або надалі оброблялися.
- *Відповідальність.* Порушення вимог законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом.

РОЗДІЛ 4. ВІДПОВІДАЛЬНІ ОСОБИ ТА СФЕРА ЗАСТОСУВАННЯ

4.1. Ця політика поширюється на всю Команду Організації, включаючи осіб з повною трудовою зайнятістю, неповною зайнятістю або тимчасових працівників, всіх підрядників, замовників, партнерських організацій, що співпрацюють з Організацією в процесі реалізації проектів чи організаційної діяльності, усіх, хто надає послуги за договором та опосередковано на бенефіціарів та інші сторони, які є учасниками фінансових чи інших відносин із Організацією.

4.2. Директорка Організації приймає стратегічне рішення щодо збору, обробки, зберігання та передачі персональних даних, конфіденційності та захисту інформаційної безпеки.

4.3.Відповідальна особа з питань моніторингу та оцінки, призначена директоркою наказом відповідає за забезпечення виконання цієї політики щодо безпечного та правильного збирання, зберігання, обробку та передачу персональних даних, конфіденційності та інформаційної безпеки, відповіді на запити, включаючи розробку та впровадження політик та процедур інформаційної безпеки. До моменту призначення окремої відповідальної особи ці функції виконує директорка Фонду.

4.4. Відповідальна особа з питань моніторингу та оцінки може за погодженням з директоркою делегувати окремі функції зі зберігання, обробки та передачі персональних даних іншим членам команди, оформивши відповідне доручення або наказ директорки.

4.5. Відповідальна особа з питань моніторингу та оцінки відповідає за ознайомлення членів Команди з цією Політикою, а також вживає заходів з підвищення обізнаності Команди Організації щодо захисту та безпеки в обробці та зберіганні персональних даних. До моменту призначення окремої відповідальної особи ці функції виконує директорка Фонду.

4.6. Директорка Фонду, Наглядова рада, керівники напрямів, координатори програм, проєктні менеджери, керівники функціональних відділів та інші зобов'язуються вживати ефективних заходів щодо збирання, обробки та зберігання персональних даних, конфіденційності та не можуть без письмового дозволу відповідальної особи з питань моніторингу та оцінки та директорки Організації передавати персональні дані інших сторонам за їх запитом.

4.7. Встановлення програмного забезпечення, антивірусних програм, оновлення операційних систем на всіх мережевих пристроях в Організації виконує виключно залучений системний адміністратор або відповідальна особа, зазначена у пункті 4.3, за погодженням з Директоркою Фонду. У разі залучення зовнішнього системного адміністратора він зобов'язаний підписати угоду про конфіденційність (NDA) до початку роботи з інформаційними системами Організації.

4.8. Системний адміністратор або відповідальна особа, зазначена у пункті 4.3, не пізніше ніж 1 раз на півроку має проводити перевірку оновлення операційних систем, програмного забезпечення для забезпечення максимального рівня безпеки Організації, а також забезпечувати захист мережевого з'єднання шляхом використання зашифрованих протоколів, фаєрволів та інших технологій захисту.

4.9. Директорка забезпечує нагляд та робочий контроль обробки персональних даних Організації, конфіденційності та інформаційної безпеки. Директорка виконує функції відповідальної особи з захисту персональних даних (Data Protection Officer — DPO) відповідно до вимог GDPR: здійснює незалежний нагляд за дотриманням законодавства про

захист персональних даних, є точкою контакту для суб'єктів персональних даних та контролюючих органів.

4.10. Розмежування функцій між відділом моніторингу та оцінки (M&E) і функцією DPO: відділ M&E відповідає за операційну діяльність зі збору, обробки та зберігання персональних даних; Директорка Організації здійснює незалежний нагляд та контроль за дотриманням вимог захисту персональних даних як DPO, що забезпечує відсутність конфлікту інтересів відповідно до вимог статті 38 GDPR. Наглядова рада здійснює загальний контроль за дотриманням цієї Політики.

РОЗДІЛ 5. КОНФІДЕНЦІЙНІСТЬ, ЗБЕРЕЖЕННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ ОРГАНІЗАЦІЇ

5.1. Членам Команди для робочих цілей використовуються корпоративні облікові записи Організації. Використання особистих поштових скриньок (@gmail.com або інших особистих акаунтів) для обробки персональних даних бенефіціарок та конфіденційної інформації Організації забороняється.

5.2. Член Команди Організації отримує відповідні інструкції та доступ до робочої пошти у перший робочий день. Після отримання пошти працівник матиме доступ до хмарних технологій Організації таких як гугл-диск Фонду та інші, де використовується принцип найменшого можливого доступу (Least Privilege), де кожному користувачеві надаються тільки ті привілеї та рівень доступу, які необхідні для виконання його обов'язків.

5.3. Члени команди повинні використовувати адресу робочої електронної пошти лише для комунікації в рамках виконання своїх обов'язків, пов'язаних з діяльністю фонду.

5.4. Для запобігання несанкціонованого доступу до облікових записів Google використовується двофакторна авторизація (MFA). При необхідності передачі конфіденційної інформації електронною поштою, слід використовувати дворівневе шифрування для забезпечення безпеки передачі даних згідно з налаштуваннями електронної пошти.

5.5. Члени Команди з моменту отримання робочої електронної пошти Організації повинні дотримуватись вимог до конфіденційності інформації, розповсюдження якої виконується через цей канал. Вони не повинні розголошувати конфіденційну інформацію третім особам без належних дозволів відповідальної особи, зазначеної у пункті 4.3, та Директорки Організації.

5.6. Члени команди Організації при отриманні робочого комп'ютера (ноутбука, планшета тощо) мають самостійно або за викликом системного адміністратора налаштувати комп'ютер механізмами

авторизації та аутентифікації для доступу до мережі Організації та встановлення захисту.

5.7. Для забезпечення конфіденційності інформації на комп'ютері проводиться шифрування носія за допомогою BitLocker. Резервний ключ зберігається у захищеному хмарному сховищі організації, доступ до якого визначається наказом Директорки.

5.8. Регулярне резервне копіювання інформації проводиться для запобігання втрати даних. Резервні копії зберігаються в безпечному місці, віддаленому від основного місця зберігання. Операційні бази даних копіюються не рідше одного разу на добу; хмарні сховища (Google Drive або OneDrive) — не рідше одного разу на квартал.

5.9.При публікації будь-якої інформації на публічних ресурсах, необхідно дбати про збереження конфіденційності персональних даних та конфіденційної інформації Організації. За це відповідає зазначена особа з пункту 4.3. Це стосується сторінок Організації в соціальних мережах (фейсбук, телеграм-каналів тощо).

5.10. Доступ до публічних ресурсів, де розміщується інформація Організації, обмежений і доступний лише відповідальним особам, які мають на це повноваження. Відповідальна особа, зазначена у пункті 4.3, періодично перевіряє список користувачів-адмінів соціальних сторінок та інших спільних ресурсів (групи, канали тощо).

5.11. Будь-яка інформація, яка стала відома членам команди Організації, у зв'язку з виконанням обов'язків за договором із Організацією, і розголошення якої може нанести шкоду другій Стороні, є комерційною таємницею і не підлягає розголошенню третім особам або опублікуванню без попередньої згоди на це іншої сторони. За розголошення вказаної інформації винна сторона несе відповідальність, передбачену діючим законодавством України.

5.12. Конфіденційною вважається у тому числі інформація, яка складає дійсну або потенційну комерційну цінність для Організації та є невідомою третім особам, і по відношенню до якої Організація вживає заходи щодо охорони її конфіденційності, а також інша інформація, яка не є комерційною таємницею, але відносно якої Організацією було заявлено, що вона є конфіденційною.

5.13. Члени колективу зобов'язуються протягом строку дії договору із Організацією та протягом 5 років після його припинення не розголошувати та не розкривати третім особам конфіденційну інформацію, надану їм Організацією, та не використовувати її з будь-якою іншою метою, крім тієї, для якої така інформація була надана Організацією, без отримання попередньої письмової згоди Організації. Організація залишає за собою право у разі необхідності контролювати

використання членами команди конфіденційної інформації та її збереження.

5.14. Члени колективу та Організація зобов'язуються дотримуватися конфіденційності переговорів, листування та інших дій, пов'язаних з договірними умовами, та не розголошувати таку інформацію третім особам без письмової згоди іншої сторони.

РОЗДІЛ 6. БАЗИ ПЕРСОНАЛЬНИХ ДАНИХ ВЛАСНИКОМ, ЯКИХ Є ОРГАНІЗАЦІЯ

6.1. Обробка персональних даних Організацією здійснюється для реалізації програм та проєктів Організації, захисту бенефіціарів та членів Команди Організації та інших цілей визначеними законодавством України і вимогам Загального регламенту про захист персональних даних (GDPR).

6.2. Підставами виникнення права на використання персональних даних є:

- згода суб'єкта персональних даних на обробку його персональних даних письмово чи за допомогою електронних засобів *(Додаток 1)*;
- дозвіл на обробку персональних даних, наданий Організації відповідно до законодавства України та вимогам Загального регламенту про захист персональних даних (GDPR) виключно для здійснення його повноважень.

6.3. Організація володіє та обробляє такі бази персональних даних:

- База даних бенефіціарів, яка містить основну інформацію про бенефіціарів фонду, включаючи ім'я, прізвище, контактні дані, інформацію про отримувану підтримку тощо.
- Метою оброблення бази персональних даних бенефіціарів є: надання послуг та допомоги бенефіціарам у межах програм та проєктів Організації; оцінка потреб та моніторинг якості отриманої допомоги; звітність перед донорами та партнерами у знеособленому або кодованому вигляді відповідно до Розділу 10 цієї Політики; виконання програмних та грантових зобов'язань Організації.
- База персональних даних членів команди Організації. У базі персональних даних членів команди Організації міститься інформація про Прізвище, Ім'я, по-батькові, дату та місце народження, домашній та мобільний телефон, електронну адресу, місце реєстрації, паспортні дані, реєстраційний номер облікової картки платника податків, освіту, сімейний стан, дітей, громадянство, наявність закордонного паспорту, наявність та категорію водійських прав, наявність судимості, дані про досвід

роботи, та інші дані за потребою. Метою оброблення бази персональних даних членів команди Організації є ведення кадрового діловодства, підготовка статистичної та адміністративної інформації з питань персоналу, реалізація прав та обов'язків у сфері трудових правовідносин і соціального захисту відповідно до законодавства України

6.4. Володіючи базою персональних даних бенефіціарів та членів команди Організації, Організація зобов'язується використовувати ці дані тільки для визначених цілей, зазначених у статуті або інших правових документах фонду, і згідно з принципами законності, справедливості та прозорості.

6.5. Організація не буде передавати персональні дані бенефіціарів та членів команди Організації третім особам без належних правових підстав, таких як згода бенефіціарів або законні вимоги відповідних органів.

6.6. Передачі персональних даних третім особам Організація робить виключно за наказом Директорки Організації та письмовою згодою відповідальної особи, зазначеної у пункті 4.3 цієї Політики.

6.7. Підставою передачі персональних даних має бути укладена угода або письмово зафіксовані інші механізми, що гарантують адекватний рівень захисту цих даних та забезпечують дотримання вимог законодавства про захист персональних даних України та вимог Загального регламенту про захист персональних даних (GDPR).

РОЗДІЛ 7. ОБМЕЖЕНИЙ ДОСТУП ДО ПЕРСОНАЛЬНИХ ДАНИХ

7.1. Організація забезпечує обмежений доступ до персональних даних бенефіціарів та членів команди Організації тільки співробітникам та іншим особам, які мають необхідний письмовий дозволений доступ до таких даних від Директорки Організації та відповідальної особи, яка зазначена у пункті 4.3. даної Політики.

7.2. Доступ до персональних даних надається лише в межах, необхідних для виконання визначених завдань та обов'язків в реалізації проєктів та програм Організації.

7.3. Відповідальна особа, яка зазначена у пункті 4.3. даної політики розробляє та оновлює навчання та інструктаж щодо використання та обробки персональних даних. 7.4. Організація забезпечує регулярне навчання та інструктаж свого персоналу щодо використання та обробки персональних даних відповідно до вимог законодавства та політик Організації не рідше ніж 1 раз на півроку. Відповідальність за постійне навчання та підвищення кваліфікації членів команди Організації покладається на особу, зазначену у пункті 4.3 цієї Політики.

7.5. Персонал Організації, який має доступ до персональних даних бенефіціарів та членів команди Організації, зобов'язується дотримуватися конфіденційності та виконувати всі необхідні заходи безпеки для захисту цих даних згідно цієї Політики українського законодавства та Загального регламенту про захист персональних даних (GDPR).

7.6. Права суб'єктів персональних даних:

- Суб'єкти персональних даних мають право на захист своїх персональних даних та використання їх відповідно до законодавства та цього положення.
- Суб'єкти персональних даних мають такі права:

  а) Право на інформацію: Суб'єкти персональних даних мають право бути інформованими про те, що їхні персональні дані збираються та обробляються, цілі обробки, категорії отримувачів даних та правову підставу для обробки згідно *Додатку 1*.

  б) Право на доступ: Суб'єкти персональних даних мають право отримувати доступ до своїх персональних даних, які зберігаються в базі персональних даних Організації, і отримувати копії цих даних подавши відповідний письмовий запит на особу, яка зазначена у пункті 4.3.

  в) Право на виправлення: Суб'єкти персональних даних мають право вимагати виправлення неправдивих або недостовірних персональних даних, які стосуються їх.

  г) Право на вилучення: Суб'єкти персональних даних мають право вимагати видалення своїх персональних даних з бази персональних даних Організації у разі, коли ці дані більше не потрібні для визначених цілей або якщо обробка їх незаконна.

  д) Право на обмеження обробки: Суб'єкти персональних даних мають право обмежити обробку своїх персональних даних у певних ситуаціях, зокрема, якщо обробка є незаконною або суб'єкт персональних даних заперечує проти обробки. е) Право на перенесення даних: Суб'єкти персональних даних мають право отримати свої персональні дані, які вони надали Організації, у структурованому, звичайно використовуваному та машинночитаному форматі, а також передати ці дані іншому володарю персональних даних без перешкоди з боку Організації, якщо обробка ґрунтується на згоді або укладеному договорі та здійснюється автоматизованим способом.

  ж) Право на відкликання згоди: У разі, коли обробка персональних даних здійснюється на підставі згоди суб'єкта даних, суб'єкт має

право в будь-який час відкликати свою згоду. Відкликання згоди не впливає на законність обробки, здійсненої до відкликання згоди.

з) Право на подання скарги: Суб'єкти персональних даних мають право подавати скарги до відповідних контролюючих органів, якщо вони вважають, що їхні права в сфері захисту персональних даних порушені.

і) Інші права: Суб'єкти персональних даних також мають інші права, передбачені законодавством про захист персональних даних.

7.7. Застосування прав суб'єктів персональних даних здійснюється шляхом звернення до Організації згідно Статті 16 Закону України «Про захист персональних даних» Організація зобов'язана забезпечити можливість здійснення цих прав та відповідно реагувати на запити суб'єктів персональних даних у межах вимог законодавства.

РОЗДІЛ 8. ПОРЯДОК ОБРОБЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ

8.1. Оброблення персональних даних здійснюється відповідно до вимог законодавства, принципів конфіденційності та безпеки персональних даних, а також вимог Загального регламенту про захист персональних даних (GDPR).

8.2. Персональні дані збираються та обробляються згідно дозволу встановленої форми (*додаток 1*).

8.3. Оброблення персональних даних може здійснюватися з використанням автоматизованих засобів, які використовує Організація (CRM-системи тощо), а також без автоматизованих засобів (зберігання письмових дозволів в офісі тощо).

8.4. Організація забезпечує виконання належних заходів для захисту персональних даних від несанкціонованого доступу, випадкового втрати або пошкодження, знищення, зміни, поширення або незаконної обробки постійно оновлюючи безпеку автоматизованих засобів зберігання персональних даних та безпечне і захищене місце в офісі, архіві Організації для не автоматизованих засобів засобів зберігання персональних даних.

8.5. Здійснення обробки персональних даних може здійснюватися Організацією або за її дорученням третіми особами на підставі укладених угод або на підставі законних підстав, визначених законодавством.

8.6. Організація забезпечує зберігання персональних даних бенефіціарів не менше 5 (п'яти) років після завершення проєкту, в рамках якого вони були зібрані, якщо грантовий договір або законодавство не передбачають більшого строку. Після закінчення строку зберігання дані знищуються у безпечний спосіб.

8.7. Припинення оброблення персональних даних може здійснюватися за ініціативою суб'єкта персональних даних, за письмовим запитом контролюючих органів або у разі виконання законних вимог, визначених законодавством.

8.8. Передача персональних даних третім особам може здійснюватися лише у випадках, передбачених законодавством, договором реалізації проєкту та відповідно до вимог забезпечення конфіденційності та безпеки персональних даних.

8.9. Організація зобов'язана здійснювати реєстрацію процесів оброблення персональних даних, зокрема ведення реєстру обробки персональних даних та інших необхідних документів, відповідно до вимог законодавства.

8.10. У разі порушення безпеки персональних даних, що може призвести до несанкціонованого доступу, втрати, зміни або пошкодження таких даних, Організація зобов'язана повідомити відповідний контролюючий орган протягом 72 годин з моменту виявлення порушення, а також суб'єктів персональних даних — без невиправданої затримки, відповідно до вимог статті 33–34 GDPR та чинного законодавства України.

8.11. Організація забезпечує належні умови для здійснення прав суб'єктів персональних даних, зокрема прав на доступ до персональних даних, виправлення неправдивих або недостовірних даних, вилучення даних тощо.

8.11-1. У разі виявлення або підозри на порушення безпеки персональних даних застосовується такий порядок дій:

1. Особа, яка виявила інцидент, негайно повідомляє відповідальну особу (п. 4.3) та Директорку Фонду.
2. Відповідальна особа протягом 24 годин проводить первинну оцінку масштабу інциденту та фіксує його у журналі інцидентів.
3. Якщо інцидент може призвести до ризику для прав суб'єктів даних — Директорка забезпечує повідомлення контролюючого органу протягом 72 годин відповідно до п. 8.10.
4. За потреби — повідомляються суб'єкти персональних даних без невиправданої затримки.
5. За результатами інциденту складається звіт із висновками та рекомендаціями щодо запобігання повторенню

РОЗДІЛ 9. ЗБІР ТА ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ

9.1. У даній політиці дитина означає особу, яка не досягла 18 років.

9.2. Організація збирає та обробляє персональні дані дітей виключно для цілей надання необхідної підтримки, допомоги та послуг, пов'язаних із

діяльністю організації. Дані можуть використовуватися для оцінки потреб дитини, розробки індивідуальних програм підтримки, моніторингу прогресу та звітності.

9.3. Організація збирає персональні дані дітей тільки за згодою батьків або законних опікунів. До отримання такої згоди Команда Організації не збирає, не використовує чи не розкриває персональні дані дітей.

9.4. Типи даних, що збираються у дітей:

- Ім'я, дата народження, контактна інформація батьків або опікунів.
- Інформація про здоров'я, включаючи медичні діагнози та історію лікування.
- Інші дані, необхідні для надання відповідних послуг.

9.5. Обробка даних:

- Дані обробляються тільки уповноваженими співробітниками, які мають безпосереднє відношення до надання послуг дитині.
- Дані використовуються виключно в межах діяльності Організації та не передаються третім особам без попередньої згоди батьків або опікунів.

9.6. Персональні дані дітей зберігаються тільки стільки, скільки необхідно для досягнення цілей їх обробки. Ми застосовуємо належні технічні та організаційні заходи для захисту даних від несанкціонованого доступу, втрати або розкриття.

9.7. Права батьків та опікунів:

- Батьки або законні опікуни мають право на доступ до персональних даних своєї дитини, право вимагати їх виправлення, видалення або обмеження обробки.
- Для реалізації цих прав батьки або опікуни можуть звернутися до нашої організації за контактними даними, вказаними на сайті чи соціальних мережах з відміткою - Дані про дитину_батьки/опікун.

9.8. У разі необхідності передачі даних третім сторонам (наприклад, медичним установам) Організація забезпечує, щоб це відбувалося лише з дозволу батьків або опікунів і згідно з чинним законодавством.

9.9. Організація приділяє особливу увагу захисту даних дітей в онлайн середовищі. Онлайн сервіси Організації мають належні заходи безпеки для захисту даних дітей.

РОЗДІЛ 10. КОДУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ БЕНЕФІЦІАРОК

10.1. Кодування персональних даних є добровільним механізмом додаткового захисту, який Організація пропонує бенефіціаркам. Кодування означає, що замість імені бенефіціарки у базі даних та в усіх

документах Організації і звітах для донорів використовується унікальний буквено-цифровий код. Застосування кодування є виключно правом бенефіціарки, а не обов'язком.

10.2. **Добровільність.** Добровільність кодування.

- Бенефіціарка самостійно приймає рішення про кодування своїх персональних даних.
- Рішення про кодування або відмову від нього фіксується у формі згоди (Додаток 1) і не впливає на доступ до послуг Організації.
- Бенефіціарка може змінити своє рішення щодо кодування в будь-який момент, звернувшись до відповідальної особи, зазначеної у п. 4.3 цієї Політики.

10.3. **Ключ кодування.** Код бенефіціарки формується за єдиним алгоритмом: 3 перші букви прізвища + 2 перші букви імені + 2 перші букви по батькові + 2 перші цифри дня народження + 2 перші цифри місяця + 2 останні цифри року + буква «ж» (жінка) або «ч» (чоловік). Наприклад: МерОлАн051072ч. Порядок роботи з кодом:

- Ключ кодування зберігається окремо від бази даних із кодами — у захищеному місці з обмеженим доступом.
- Доступ до коду мають усі співробітники/ці, які безпосередньо працюють з кодуванням клієнток: кейс-менеджерки, соціальні працівники/ці та інші уповноважені особи, а також Директорка Фонду. Перелік уповноважених осіб затверджується наказом Директорки.
- При зміні складу персоналу, який працює з кодами, Директорка наказом оновлює перелік уповноважених осіб.
- Ключ кодування не передається третім особам, партнерам або донорам за жодних обставин.

10.4. **Що передається донорам.** Організація передає донорам та партнерам виключно знеособлені (кодовані) дані — без можливості ідентифікації особи бенефіціарки. Передача будь-яких даних, що дозволяють встановити особу кодованої бенефіціарки, заборонена без її письмової згоди.

10.5. **Права кодованої бенефіціарки.** Кодована бенефіціарка зберігає всі права суб'єкта персональних даних, визначені у розділі 7 цієї Політики, зокрема:

- право на доступ до своїх персональних даних — шляхом звернення до відповідальної особи (п. 4.3) з підтвердженням своєї особи;
- право на виправлення, вилучення або обмеження обробки своїх даних;

- право відкликати згоду на кодування та перейти до стандартного режиму зберігання даних;
- право знати хто має доступ до ключа кодування та як захищені її дані.

10.6. **Зберігання та звітність.** Інформація про систему кодування, включаючи перелік осіб із доступом до ключа та журнал звернень до ключа, зберігається не менше 5 років та надається Наглядовій раді або донору на запит у знеособленому вигляді.

10.7. **Некодовані бенефіціарки.** Бенефіціарки, які не обрали кодування, захищаються стандартними заходами відповідно до розділів 5–8 цієї Політики та Закону України « Про захист персональних даних».

РОЗДІЛ 11. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

11.1. Ця Політика нерозривно пов'язана з іншими політиками Організації.

11.2. Всі зміни та доповнення до цієї Політики вносяться шляхом викладення її в новій редакції або внесення змін у вигляді окремого додатку.

11.3. Після затвердження нової редакції Політики попередня втрачає чинність.

11.4. З інших питань, які не врегульовані цією Політикою, слід керуватися чинним законодавством та GDPR.

11.5. Ця Політика переглядається не рідше ніж один раз на два роки або раніше - у разі змін у законодавстві України чи вимогах GDPR, зміни донорських вимог або суттєвих змін в операційній діяльності Організації. Перегляд ініціює відповідальна особа, зазначена у пункті 4.3, та затверджує Директорка за погодженням з Наглядовою радою.

Директорка
БО «БФ «Позитивні жінки Одеса» **Лілія ГРИНЮК**

Додаток 1

ЗГОДА

на обробку персональних даних (може бути інтегрована в інші документи Організації, де бенефіціар ставить свій підпис та поінформований про збір даних)

Підписуючи цей документ, Я _____надаю свою згоду на:

● збір, реєстрацію, зберігання, використання та інші форми обробки моїх персональних даних, у тому числі з використанням інформаційних систем,

● моніторинг, а також на проведення фотофіксації будь-яких необхідних особистих документів, що надані мною у паперовому вигляді або у форматі фотокопії.

Згода надається у повному обсязі, без додаткового письмового повідомлення для оформлення, надання та проведення моніторингу якості отриманої допомоги та інших цілей, пов'язаних із отриманою допомогою.

Я також надаю згоду на передачу та обробку моїх персональних даних третім особам - донорам, партнерським організаціям та верифікаторам - виключно у знеособленому або кодованому вигляді та лише з метою проведення перевірки і оцінки якості отриманої допомоги відповідно до грантових зобов'язань Організації

Опція кодування (поінформуйте бенефіціарку про можливість кодування відповідно до Розділу 10 Політики та запропонуйте обрати один із варіантів) □ *Я обираю кодування моїх персональних даних.*

□ Я не обираю кодування і погоджуюсь на стандартний режим зберігання даних. Я розумію, що моє рішення не впливає на доступ до послуг Організації і можу бути змінене в будь-який момент. Своїм підписом я підтверджую, що мене повідомлено про мої права як суб'єкта персональних даних, які визначені в ст. 8 Закону України «Про захист персональних даних», а також про мету збору цих даних та осіб, яким ці дані передаються.

Дата:_____ **Підпис:**_____