Історія змін:

Версія	*Назва*	*Підготовано:*
V3.0	*Політика захисту даних*	*Січень 2026*

Зміст

1. Мета політики

1. БО БФ «Ранок Відродження» (далі - Організація) дуже серйозно ставиться до захисту приватності. Повага до приватності та захист персональних даних є фактором довіри, цінністю, яким Організація приділяє особливу увагу, зосереджуючись на дотриманні фундаментальних прав і свобод. Ця Політика захисту даних ілюструє прихильність Організації до конфіденційності та захисту персональних даних.
2. Метою цієї Політики є викладення основних принципів, пов'язаних із захистом персональних даних, які Організація впроваджує в рамках усієї своєї діяльності.

2. Сфера використання

1. Ця політика поширюється на всіх співробітників та членів керівництва Організація.
2. Положення цієї політики також можуть бути застосовані до будь-якої особи, яка працює в організації, що виконує місії для Організація.
3. Ця Політика також застосовується до всіх персональних даних, що обробляються через:

   офіційний веб-сайт Організації;

   електронні форми реєстрації;

   систему електронної черги бенефіціарів;

   онлайн-анкети для отримання гуманітарної допомоги;

   електронні поштові скриньки Організації;

   CRM або інші цифрові інструменти управління даними.

3. Визначення

Для цілей цієї Політики наведені нижче терміни мають такі значення:

- *"Одержувач даних":* означає фізичну або юридичну особу, державний орган, департамент або інший орган, який отримує розкриття персональних даних, незалежно від того, чи є він третьою стороною чи ні;
- *"Персональні дані":* означає будь-яку інформацію, що стосується ідентифікованої фізичної особи або фізичної особи, яку можна ідентифікувати; "фізична особа, яку можна ідентифікувати" вважається "фізичною особою", якщо її можна ідентифікувати, прямо чи опосередковано, зокрема, шляхом посилання на ідентифікатор, такий як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор, або на один чи більше елементів, характерних для її фізичної, фізіологічної, генетичної, психологічної, економічної, культурної чи соціальної ідентичності;
- *"Співробітники"*: згідно з умовами цієї політики, термін "співробітники" означає будь-яку особу, яка працює в Організації.
- *"Суб'єкт даних":* означає фізичну особу, яку можна ідентифікувати прямо чи опосередковано, зокрема, шляхом посилання на ідентифікатор, такий як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або один чи більше елементів, характерних для її фізичної, фізіологічної, генетичної, психологічної, економічної, культурної чи соціальної ідентичності. Для цілей цієї політики суб'єкт даних визначається як фізична особа, чиї персональні дані обробляються Організацією.

- *"Застосовне законодавство"*: означає чинне законодавство, що стосується захисту приватного життя у зв'язку з обробкою персональних даних, зокрема Закон України "Про захист персональних даних" № 2297-VI
- *"Третя особа"*: означає фізичну або юридичну особу, орган державної влади, відомство або орган, відмінний від суб'єкта даних, який є суб'єктом операції обробки, контролера даних, субпідрядника та осіб, які перебувають під безпосереднім керівництвом контролера або субпідрядника, уповноважених обробляти персональні дані.
- *"Обробка"*: означає будь-яку операцію або набір операцій, що здійснюються з використанням або без використання автоматизованих процесів і застосовуються до Персональних даних або наборів Персональних даних, таких як збір, запис, організація, структурування, зберігання, адаптація або зміна, витяг, пошук, консультація, використання, повідомлення шляхом передачі, поширення або будь-якої іншої форми надання доступу, зіставлення або взаємозв'язку, обмеження, видалення або знищення.

4. Дотримання політики

1. Співробітники зобов'язуються дотримуватися принципу обробки персональних даних у будь-який час при виконанні своїх обов'язків.
2. У разі нової обробки персональних даних співробітники Організації повинні дотримуватися принципів, викладених нижче.

5. Законність обробки даних

1. Кожна обробка персональних даних, яку здійснює Організація, повинна відповідати/дотримуватися чинного законодавства. Персонал Організації виконує свої обов'язки відповідно до правових зобов'язань, що стосуються операцій з обробки.
2. При обробці персональних даних, які відповідають законним інтересам Організації, повинні бути застосовані спеціальні заходи захисту для забезпечення оптимального захисту приватного життя.

6.Мета обробки даних

1. Мета операцій з обробки даних, що здійснюються Організацією, повинна бути заздалегідь визначеною, законною, чіткою та сумісною з місіями, які виконує Організація.
2. Персональні дані не повинні використовуватися у спосіб, несумісний з цілями, спочатку визначеними для кожної операції обробки.

7. Точність даних

1. Визначені та заздалегідь встановлені цілі дозволяють оцінити релевантність Персональних даних, які збирає Організація. Збираються та обробляються лише ті дані, які є адекватними та суворо необхідними для досягнення цих цілей.
2. Організація зобов'язується обробляти тільки точні, повні та актуальні дані. За цих умов Організація залишає за собою право вимагати від суб'єктів даних підтвердження точності їхніх персональних даних.

8. Збереження даних

1. Відповідно до мети обробки, період зберігання даних необхідний для визначення діяльності відповідно до чинного законодавства.
2. Персональні дані зберігаються не довше, ніж це необхідно відповідно до заздалегідь визначених цілей.
3. Персональні дані зберігаються доти, доки цього вимагає чинне законодавство.
4. З будь-яких питань щодо зберігання персональних даних, будь ласка, звертайтеся за наступною адресою: **complaints@newdawn.org.ua**

9. Інформування суб'єктів

1. Організація повинна надавати чітку, повну, легкодоступную та зрозумілу інформацію для обробки персональних даних.
2. У зв'язку з цим будь-який суб'єкт даних повинен бути проінформований про наступне:

   - Мета обробки, для якої призначені дані;
   - Одержувачі даних або категорії одержувачів даних;
   - Права суб'єктів даних щодо обробки їх персональних даних, як зазначено в цій політиці;
   - Ідентифікаційні дані контролера та, за необхідності, його представника;

10.Права суб'єктів даних та процедури їх реалізації

1. Організація зобов'язується впроваджувати технічні та організаційні заходи, які дозволять суб'єктам даних користуватися наступними правами:

   - право доступу: право суб'єкта даних бути проінформованим і вимагати розкриття його персональних даних в зрозумілому форматі;
   - право на виправлення: право суб'єкта даних на виправлення персональних даних, якщо вони вважаються неточними;
   - право на видалення: право суб'єкта даних на видалення його/її персональних даних;
   - право на обмеження: право суб'єкта даних на обмеження обробки його персональних даних;
   - право на переносимість: право суб'єкта даних отримувати свої персональні дані, що стосуються його/її, у структурованому форматі;
   - право на заперечення: право суб'єкта даних заперечувати проти повної або часткової обробки його персональних даних з причин, що стосуються його конкретної ситуації;
   - кожен суб'єкт даних має право визначати вказівки щодо використання своїх персональних даних після своєї смерті.

2. Всіма вищезазначеними правами можна скористатися в будь-який час, надіславши запит електронною поштою на адресу: **complains@newdawn.org.ua**
3. За будь-яким запитом Організація залишає за собою право провести перевірку особи.
4. У разі подання скарги будь-яка зацікавлена особа може звернутися до контролюючого органу.

5. У разі запиту суб'єкта даних про вищезазначені права, Організація повинна відповісти якомога швидше в межах одного місяця.

11.Конфіденційність

11.1. Повага до конфіденційності даних, особливо при використанні будь-яких електронних засобів зв'язку, є важливою вимогою Організації.

11.2. Захист інтересів Організації вимагає від кожного дотримуватися загального та постійного зобов'язання щодо конфіденційності, розсудливості та комерційної таємниці стосовно даних, наданих Користувачеві для здійснення його професійної діяльності, зокрема соціальної, правової, фінансової, комерційної, наукової, технічної, економічної або промислової інформації, в контексті використання Інформаційних систем.

Дотримання цього зобов'язання вимагає:

- гарантувати, що така інформація не стане відомою стороннім особам;
- не привласнювати, не зберігати та не відтворювати таку інформацію для особистого використання;
- використовувати інформацію відповідно до заздалегідь визначених цілей;
- поважати правила професійної етики та розсудливості у використанні в межах Організації.

11.3. Передача конфіденційних даних може бути здійснена лише за умови отримання попереднього дозволу уповноваженої особи :

- дозвіл особи, яка надає дані;
- дотримання безпечної процедури;

- або у випадку витребування персональних даних уповноваженою особою правоохоронних органів за наявності відповідного рішення суду або підтвердження повноважень.

11.4. Організація вимагає від будь-якого субпідрядника, якому було довірено персональні дані, забезпечити належні гарантії захисту конфіденційності персональних даних.

12. Безпека

12.1. Організація зобов'язується, в межах своїх можливостей, вживати всіх необхідних заходів обережності для збереження безпеки Персональних даних і, зокрема, для запобігання їх спотворенню, знищенню або передачі несанкціонованим третім особам.

12.2. Організація також вимагає підтвердження у письмовому вигляді від будь-якого субпідрядника, якому було довірено персональні дані, забезпечити належні гарантії для забезпечення безпеки персональних даних.

12.3. Тільки належним чином уповноважені одержувачі даних можуть отримати доступ до інформації, необхідної для їхньої діяльності. Права доступу надаються відповідно до принципів "найменших привілеїв" та "необхідності знати".

12.4. Організація застосовує такі технічні заходи:

- захищене HTTPS-з’єднання сайту;
- SSL-сертифікат;
- складні паролі та двофакторну аутентифікацію;
- регулярне резервне копіювання;
- шифрування носіїв інформації;
- обмеження IP-доступу (за можливості);
- антивірусний та firewall-захист;

- журналювання доступів до баз даних (покладається на обслуговуючу фірму, що володіє серверами, де зберігаються відповідні дані).

12.5. Організаційні заходи безпеки

- Підписання угод про конфіденційність співробітниками.
- Обмеження копіювання баз даних на персональні пристрої.
- Регулярне навчання персоналу щодо обробки персональних даних.
- Наявність внутрішньої процедури реагування на витік даних.

13. Обробка персональних даних через веб-сайт та систему електронної черги

13.1. Категорії персональних даних, що збираються

Через веб-сайт та електронну чергу Організація може збирати:

- ПІБ;
- контактний номер телефону;
- електронну адресу;
- місце проживання;
- статус ВПО;
- склад домогосподарства;
- дані документів (за потреби);
- інші дані, необхідні для надання допомоги.

У разі обробки даних щодо соціального статусу, здоров'я або інших чутливих категорій, Організація застосовує підвищені заходи захисту.

13.2. Правова підстава обробки

Обробка здійснюється на підставі:

- згоди суб'єкта персональних даних;

- виконання статутної діяльності Організації;
- виконання грантових зобов'язань;
- законного інтересу Організації щодо надання гуманітарної допомоги;
- виконання вимог законодавства України.

Згода суб'єкта надається шляхом встановлення відповідної відмітки (checkbox) під час заповнення онлайн-форми.

13.3. Інформування суб'єкта при зборі даних онлайн

Перед відправкою форми електронної черги суб'єкту надається інформація про:

- мету збору даних;
- обсяг даних;
- строк зберігання;
- одержувачів даних (донори, партнери);
- права суб'єкта;
- контактні дані відповідальної особи з питань захисту даних.

13.4. Зберігання та локалізація серверів

Персональні дані, зібрані через веб-сайт та електронну чергу:

- зберігаються на захищених серверах;
- не передаються третім особам без правової підстави;
- можуть зберігатися на серверах, розташованих за межами України, якщо це передбачено технічними рішеннями (з дотриманням належного рівня захисту).

13.5. Обмеження доступу

Доступ до електронної бази бенефіціарів мають лише:

- HR (у частині кадрових даних);

- менеджери проєктів;
- фінансовий відділ (за потреби);
- керівник організації;
- відповідальна особа з обробки даних.

Доступ надається відповідно до принципів:

✔ «необхідності знати»

✔ «найменших привілеїв»

Затверджено та підписано

Керівник **Юлія ПОГРЕБНА**

Відповідальна особа **Наталія СМІРНОВА**

Додаток 1. Інструкція зі строків зберігання документації БО БФ "Ранок Відродження"

1. Мета

Цей додаток встановлює строки зберігання різних типів документації, що обробляються та зберігаються у межах діяльності Фонду, відповідно до законодавства України, податкових норм, вимог донорів, а також Політики захисту персональних даних.

2. Загальні принципи

- Зберігання документів здійснюється з дотриманням Закону України «Про захист персональних даних» № 2297-VI, Закону України «Про архівну справу та діловодство» № 3814-XII, Податкового кодексу України.
- Після завершення строку зберігання документи мають бути знищені або архівовані відповідно до політики Фонду.
- Для збереження даних використовується безпечне середовище (електронне чи фізичне архівне приміщення).

3. Таблиця строків зберігання документації

Тип документації	Строк зберігання	Підстава / коментар
Проєктна документація	**10 років**	Згідно з вимогами донорів
Фінансова звітність	**3–5 років**	Податковий кодекс України, ст. 44
Первинна бухгалтерська документація	**3 роки**	Після подання звітності (Порядок №1007)
Документи з кадрових питань (особові справи)	**75 років**	Закон України «Про Нац. архівний фонд»
Табелі обліку робочого часу	**3 роки**	Законодавство про працю
Договори з контрагентами	**3 роки після завершення дії**	Цивільний кодекс України
Документація з державної реєстрації	**Постійно**	Архівне законодавство України

Акти приймання-передачі гуманітарної допомоги	**5 років**	Вимоги донорів та внутрішні протоколи
Документи, що містять персональні дані	**До досягнення мети обробки + 1 рік**	Або до закінчення строку дії договору / проєкту
Скарги, запити, анкети бенефіціарів	**3 роки**	GDPR / Закон України про персональні дані
Дані про облік волонтерів	**3 роки після останнього залучення**	За згодою або відповідно до умов контракту
Заяви на відпустку, лікарняні	**3 роки**	Законодавство про працю
Внутрішні політики та процедури	**До втрати актуальності + 3 роки**	Архівна практика

4. Відповідальні особи

- HR-менеджер: зберігає документи, що стосуються персоналу.
- Юрист: контролює строки зберігання договорів, реєстраційних даних.
- Фінансовий асистент: відповідає за зберігання фінансових документів.
- Менеджери проєктів: ведуть архів проєктної звітності.
- Організатор діловодства: здійснює контроль за дотриманням цієї інструкції.

5. Завершення строку зберігання

- Документи, строк зберігання яких сплив, підлягають знищенню або передачі до архіву відповідно до акту.
- Знищення документів із персональними даними має здійснюватися із забезпеченням їх повної недоступності (наприклад, подрібнення, очищення диску).

Затверджено та підписано

Керівник **Юлія ПОГРЕБНА**

Відповідальна особа **Наталія СМІРНОВА**

Додаток 2. Реагування на порушення безпеки персональних даних

1. Загальні положення

Організація визнає, що будь-яке порушення безпеки персональних даних може створити ризики для прав і свобод суб'єктів даних, а також репутаційні, фінансові та грантові ризики для Організації.

Під порушенням безпеки персональних даних розуміється будь-яка подія, що призвела або могла призвести до:

- несанкціонованого доступу до персональних даних;
- випадкового або незаконного знищення;
- втрати;
- зміни;
- розголошення;
- передачі третім особам без правових підстав.

2. Приклади інцидентів

До інцидентів безпеки, зокрема, належать:

- злам електронної пошти співробітника;
- компрометація бази даних електронної черги;
- втрата ноутбука, флеш-носія або паперових документів;
- помилкова відправка персональних даних невірному адресату;
- несанкціоноване копіювання або фотографування баз даних;
- витік через сторонній сервіс або субпідрядника.

3. Відповідальна особа

Розпорядником інформації та відповідальною особою за координацію реагування на інциденти визначається:

Смірнова Наталія Романівна

До її повноважень належить:

- фіксація інцидентів;
- координація внутрішнього розслідування;
- взаємодія з керівником Організації;
- підготовка повідомлень донорам;
- прийняття рішення щодо інформування суб'єктів даних;
- ведення Журналу інцидентів безпеки.

4. Алгоритм реагування

Крок 1. Негайне повідомлення

Будь-який співробітник, який виявив або підозрює порушення безпеки, зобов'язаний:

- негайно повідомити Смірнову Наталію Романівну;
- не вживати самостійних дій без координації;
- зберегти всі можливі докази.

Крок 2. Фіксація інциденту

Розпорядник інформації:

- реєструє інцидент у Журналі інцидентів;
- визначає дату, час, характер події;
- оцінює категорії даних та кількість суб'єктів.

Крок 3. Оцінка ризиків

Проводиться оцінка:

- чутливості даних;
- масштабу інциденту;
- потенційних наслідків для суб'єктів;
- ймовірності використання даних третіми особами.

Крок 4. Локалізація та мінімізація шкоди

Вживаються заходи:

- блокування доступу;
- зміна паролів;
- тимчасове обмеження систем;
- відкликання доступів;
- інформування IT-підрядника (за потреби).

Крок 5. Внутрішнє розслідування

Проводиться службове розслідування для встановлення:

- причин інциденту;
- відповідальних осіб (за наявності);
- системних недоліків.

За результатами готується внутрішній звіт.

Крок 6. Повідомлення зацікавлених сторін

6.1. Повідомлення суб'єктів даних

Якщо інцидент створює високий ризик для прав і свобод суб'єктів, Організація:

- інформує відповідних осіб у розумний строк;
- роз'яснює можливі ризики;
- надає рекомендації щодо захисту.

6.2. Повідомлення донорів

У випадках, передбачених грантовими угодами або внутрішніми зобов'язаннями, Організація повідомляє донора у встановлений договором строк.

6.3. Повідомлення державних органів

У випадках, передбачених законодавством України, може здійснюватися інформування компетентного органу.

5. Документування

За кожним інцидентом формується пакет документів:

- опис події;

- оцінка ризику;
- перелік вжитих заходів;
- рекомендації щодо недопущення повторення.

Документи зберігаються у відповідності до законодавства України та Додатку 1 до цієї Політики.

6. Запобіжні заходи

Після інциденту Організація:

- переглядає процедури безпеки;
- проводить додатковий інструктаж персоналу;
- посилює технічні засоби захисту;
- за потреби оновлює Політику захисту даних.

7. Дисциплінарна відповідальність

У разі встановлення порушення співробітником правил обробки персональних даних можуть застосовуватися заходи дисциплінарного впливу відповідно до трудового законодавства та внутрішніх політик.

Затверджено та підписано

Керівник **Юлія ПОГРЕБНА**

Відповідальна особа **Наталія СМІРНОВА**