



сумська
психологічна
кризова
служба

Кризовий центр психічного здоров'я Mental Health Crisis Center

*громадська організація
non-governmental organization*

юридична адреса:

м. Суми, Україна

legal address:

e-mail: i@mhc.center

alternate e-mail: mhc.center.sumy@gmail.com

<http://mhc.center>

тел./phone: +38-050-0542-050, +38-050-613-8037

код ЄДРПОУ/EDRPOU code: 26270458

ЗАТВЕРДЖЕНО

Протоколом № 1/01 від 08.01.2026

Загальних зборів ГО «КЦПЗ»

**ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ
ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ
«КРИЗОВИЙ ЦЕНТР ПСИХІЧНОГО ЗДОРОВ'Я»
ГО «КЦПЗ»**

APPROVED BY

Protocol № 1/01 of 08.01.2026

of the General Meeting of the NGO "MHCC"

DATA PROTECTION AND CONFIDENTIALITY POLICY

**THE NON-GOVERNMENTAL ORGANIZATION
"MENTAL HEALTH CRISIS CENTER"
NGO "MHCC"**

Редакція: 2026 року

Попередня редакція: затверджена Протоколом № 4 від 08.01.2025

Дата набрання чинності цією редакцією: 08.01.2026

Дата наступного обов'язкового перегляду: 08.01.2027

Відповідальна за перегляд: Іванцова Оксана, проєктна менеджерка, уповноважена особа з питань етики, захисту та PSEA

Version: 2026

Previous version: approved by Protocol No. 4 dated 08 January 2025

Effective date of this version: 08 January 2026

Next mandatory review date: 08 January 2027

Responsible for review: Oksana Ivantsova, Project Manager, designated Ethics, Safeguarding and PSEA Focal Point

1. Мета та сфера дії

1.1. Ця Політика конфіденційності та захисту персональних даних визначає правила збору, використання, зберігання, передачі, захисту та видалення персональних даних і конфіденційної інформації у діяльності ГО «Кризовий центр психічного здоров'я» далі — Організація.

1.2. Метою Політики є:

- захист прав, приватності та гідності бенефіціарів, дітей, сімей, працівників, волонтерів, партнерів та інших осіб;
- забезпечення законної, етичної та безпечної обробки персональних даних; - мінімізація ризиків витоку, несанкціонованого доступу або неправомірного використання даних;
- забезпечення конфіденційності психологічної, соціальної, медичної, сімейної, safeguarding та іншої чутливої інформації;
- виконання вимог законодавства України, sincerity donor вимог та внутрішніх політик Організації.

1.3. Політика поширюється на:

- працівників Організації;
- керівництво;
- членів органів управління;
- волонтерів;
- консультантів;

- стажерів;
- тренерів;
- підрядників;
- партнерів;
- інших осіб, які отримують доступ до персональних даних або конфіденційної інформації в межах діяльності Організації.

1.4. Політика застосовується до всіх форматів інформації:

- паперових документів;
- електронних файлів;
- баз даних;
- електронної пошти;
- месенджерів;
- фото, відео та аудіо;
- форм реєстрації;
- кейс-файлів;
- списків учасників;
- звітів;
- нотаток консультантів;
- даних, що передаються партнерам або донорам.

1.5. Політика застосовується разом із:

- Політикою етичної поведінки;
- Політикою PSEA;
- Політикою захисту дітей;
- Механізмом зворотного зв'язку та розгляду скарг;
- Політикою щодо повідомлень про порушення;
- Антикорупційною та антишахрайською політикою;
- SOP безпеки мобільних виїздів;
- іншими внутрішніми процедурами Організації.

2. Основні терміни

2.1. У цій Політиці терміни вживаються в такому значенні:

2.1.1. Персональні дані — будь-яка інформація, що прямо або опосередковано дозволяє ідентифікувати фізичну особу.

2.1.2. Чутливі дані — інформація, розкриття або неправомірне використання якої може створити підвищений ризик шкоди для особи. До чутливих даних можуть належати дані про дитину, стан здоров'я, психологічний стан, досвід насильства, інвалідність, сімейні обставини, місце проживання, статус ВПО, контактні дані, safeguarding-випадки, PSEA-повідомлення, кейс-менеджмент або звернення по допомогу.

2.1.3. Конфіденційна інформація — будь-яка інформація, доступ до якої обмежений через її службовий, персональний, безпековий або чутливий характер.

2.1.4. Обробка даних — будь-яка дія з персональними даними, включаючи збір, запис, зберігання, використання, передачу, аналіз, оновлення, знеособлення або видалення.

2.1.5. Суб'єкт даних — фізична особа, якої стосуються персональні дані.

2.1.6. Інформована згода — добровільна згода особи на обробку її даних після отримання зрозумілої інформації про мету, обсяг, спосіб використання, можливу передачу та строки зберігання даних.

2.1.7. Знеособлення — видалення або зміна інформації, яка дозволяє прямо або опосередковано ідентифікувати особу.

2.1.8. Витік даних — випадкове або незаконне знищення, втрата, зміна, несанкціоноване розкриття або доступ до персональних даних чи конфіденційної інформації.

3. Основні принципи захисту даних

3.1. Організація дотримується таких принципів:

3.1.1. Законність, добросовісність і прозорість

Дані обробляються законно, етично, добросовісно та зрозуміло для особи.

3.1.2. Обмеження мети

Дані збираються лише для визначених, законних і конкретних цілей, пов'язаних із діяльністю Організації.

3.1.3. Мінімізація даних

Організація збирає лише ті дані, які є необхідними для надання послуг, реалізації програм, безпеки, звітності або виконання законних зобов'язань.

3.1.4. Точність

Дані мають бути, наскільки це можливо, точними та актуальними.

3.1.5. Обмеження строку зберігання

Дані зберігаються не довше, ніж це необхідно для мети їх обробки, вимог донора, законодавства або захисту прав Організації та бенефіціарів.

3.1.6. Конфіденційність і безпека

Дані захищаються від несанкціонованого доступу, втрати, пошкодження, розкриття або неправомірного використання.

3.1.7. Підзвітність

Організація документує ключові процеси обробки даних і забезпечує відповідальне поводження з інформацією.

4. Які дані може збирати Організація

4.1. Залежно від виду послуги або програми

Організація може збирати такі дані:

- ім'я та прізвище;
- дата народження або вік;
- стать;
- контактний номер телефону;
- e-mail;
- адреса або громада проживання;
- статус ВПО або належність до цільової групи;
- інформація про участь у заходах або консультаціях;
- дані про потреби в психосоціальній підтримці;
- інформація про сімейний склад;
- інформація про дітей, батьків або законних представників;
- інформація, необхідна для кейс-менеджменту;
- інформація для перенаправлення до інших служб;
- згода на участь у заходах або послугах;
- згода на фото, відео або публічні матеріали, якщо така потрібна;
- відгуки, скарги або звернення;
- дані, необхідні для донорської звітності.

4.2. Організація не збирає чутливі дані без потреби.

4.3. У випадках, пов'язаних із дітьми, психологічною допомогою, PSEA, safeguarding, насильством або іншими чутливими ситуаціями, збирається лише мінімально необхідна інформація.

5. Правові та етичні підстави обробки даних

5.1. Організація може обробляти персональні дані на таких підставах:

- інформована згода особи;
- необхідність надання послуги або допомоги;
- виконання договору або проєктних зобов'язань;
- виконання законних обов'язків;
- захист життєво важливих інтересів особи;

- законний інтерес Організації, якщо він не переважає права та свободи особи;
- вимоги донора щодо звітності, за умови мінімізації та захисту даних.

5.2. Обробка даних дітей здійснюється з урахуванням найкращих інтересів дитини, інформованої згоди батьків або законних представників, а також участі самої дитини відповідно до її віку та зрілості.

5.3. У випадках, коли існує серйозний ризик для життя, здоров'я або безпеки дитини чи іншої особи, Організація може передати необхідну інформацію відповідним службам або компетентним органам відповідно до законодавства та принципу do no harm.

6. Інформована згода

6.1. Перед збором персональних даних Організація, наскільки це можливо, пояснює особі:

- які дані збираються;
- з якою метою;
- хто матиме доступ;
- як довго дані можуть зберігатися;
- чи можуть дані передаватися партнерам або донорам;
- які права має особа;
- як відкликати згоду або поставити запитання.

6.2. Згода має бути добровільною, конкретною, інформованою та зрозумілою.

6.3. Відмова від надання необов'язкових даних не повинна автоматично призводити до відмови в основній допомозі, якщо такі дані не є необхідними для надання послуги або безпеки.

6.4. Для дітей згода отримується від батьків або законних представників, якщо інше не передбачено законом або невідкладною необхідністю захисту дитини.

6.5. Фото, відео та історії бенефіціарів використовуються лише за окремою згодою, якщо інше не передбачено законними підставами.

7. Конфіденційність у психологічній та соціальній роботі

7.1. Інформація, отримана під час психологічних консультацій, групових занять, кейс-менеджменту або іншої допомоги, є конфіденційною.

7.2. Працівники, консультанти та волонтери не мають права обговорювати інформацію про бенефіціарів з особами, які не залучені до надання допомоги або не мають службової необхідності.

7.3. Конфіденційність може бути обмежена, якщо:

- існує серйозний ризик для життя або здоров'я особи;
- існує ризик шкоди дитині;
- є загроза для інших осіб;
- інформація має бути передана відповідно до закону;
- передача необхідна для безпечного перенаправлення або надання допомоги.

7.4. У таких випадках передається лише мінімально необхідна інформація.

8. Доступ до даних

8.1. Доступ до персональних даних і конфіденційної інформації надається лише особам, яким це необхідно для виконання службових обов'язків.

8.2. Доступ може мати:

- відповідальний працівник або консультант, який надає послугу;
- проектна команда в межах службової необхідності;
- керівництво Організації;
- уповноважена особа з питань етики, захисту та PSEA;
- особи, відповідальні за звітність, фінанси або моніторинг, лише в межах необхідного;
- партнерські або спеціалізовані служби у випадку перенаправлення, за наявності підстав;
- донори, якщо це передбачено умовами проєкту, переважно у знеособленому або агрегованому вигляді.

8.3. Доступ до PSEA, safeguarding, дитячих кейсів, скарг і чутливих випадків має бути максимально обмеженим.

9. Зберігання паперових документів

9.1. Паперові документи, що містять персональні або чутливі дані, зберігаються в безпечному місці з обмеженим доступом.

9.2. Документи не повинні залишатися без нагляду у відкритому доступі.

9.3. Під час мобільних виїздів паперові списки, форми, згоди або кейс-нотатки повинні зберігатися у відповідальній особі та не передаватися стороннім особам.

9.4. Після завершення активності документи мають бути передані на безпечне зберігання відповідальній особі Організації.

10. Зберігання електронних даних

10.1. Електронні дані зберігаються у захищених файлах, папках, хмарних сховищах або пристроях із контрольованим доступом.

10.2. Організація за можливості застосовує:

- паролі;
- обмеження доступу;
- двофакторну автентифікацію;
- резервне копіювання;
- антивірусний захист;
- оновлення програмного забезпечення;
- контроль прав доступу;
- видалення доступу після завершення співпраці з працівником або консультантом.

10.3. Забороняється зберігати чутливі дані у відкритому доступі, незахищених особистих пристроях або спільних папках без обмеження доступу.

10.4. Передача файлів із персональними даними має здійснюватися безпечними каналами та лише в обсязі, необхідному для визначеної мети.

11. Використання месенджерів та електронної пошти

11.1. Месенджери та електронна пошта можуть використовуватися для службової комунікації з дотриманням конфіденційності та мінімізації даних.

11.2. Забороняється передавати через незахищені канали надмірні або непотрібні чутливі дані.

11.3. У месенджерах не слід поширювати повні списки бенефіціарів, деталі психологічних кейсів, PSEA-повідомлення, інформацію про насильство або інші чутливі дані без нагальної службової потреби.

11.4. У разі потреби передати чутливу інформацію слід використовувати мінімально необхідний обсяг даних і, за можливості, знеособлення.

12. Фото, відео та історії бенефіціарів

12.1. Фото, відео, аудіозаписи, цитати або історії бенефіціарів можуть використовуватися лише за наявності інформованої згоди, якщо інше не передбачено законом.

12.2. Для дітей потрібна згода батьків або законних представників, а також врахування думки дитини відповідно до її віку та зрілості.

12.3. Забороняється використовувати зображення або історії, які:

- принижують гідність особи;
- створюють ризик стигматизації;
- розкривають чутливу інформацію;
- можуть поставити особу або дитину під загрозу;
- демонструють дитину у вразливому або принизливому контексті;
- можуть бути використані для ідентифікації постраждалої особи без належних підстав.

12.4. Особа має право відмовитися від фото або відео без втрати доступу до послуг.

13. Передача даних партнерам, донорам та третім сторонам

13.1. Передача персональних даних третім сторонам здійснюється лише за наявності законної, договірної або операційної підстави.

13.2. Для донорської звітності Організація, наскільки це можливо, використовує:

- агреговані дані;
- знеособлені дані;
- статистичну інформацію;
- узагальнені результати.

13.3. Передача ідентифікованих персональних даних донорам або партнерам допускається лише тоді, коли це необхідно, пропорційно, безпечно та відповідає умовам проекту, згоді особи або законним вимогам.

13.4. Передача даних для перенаправлення до іншої служби здійснюється за інформованою згодою особи, крім випадків, коли існує серйозний ризик для життя, здоров'я або безпеки.

14. Знеособлення та звітність

14.1. У звітах, презентаціях, публікаціях і донорській комунікації Організація використовує знеособлені або агреговані дані, якщо немає окремої підстави для використання ідентифікованої інформації.

14.2. Приклади з практики або історії бенефіціарів мають бути змінені або знеособлені так, щоб особу неможливо було ідентифікувати без її окремої згоди.

14.3. Особлива обережність застосовується щодо дітей, осіб, які пережили насильство, осіб із психічними або психологічними труднощами, ВПО та інших вразливих груп.

15. Строки зберігання та видалення даних

15.1. Дані зберігаються лише протягом строку, необхідного для:

- надання послуг;
- виконання проекту;
- звітності перед донором;
- фінансового або юридичного обліку;
- виконання законних зобов'язань;
- захисту прав і законних інтересів Організації або бенефіціарів.

15.2. Після завершення необхідного строку дані мають бути безпечно видалені, знищені або знеособлені.

15.3. Паперові документи з персональними даними знищуються способом, який унеможливорює відновлення інформації.

15.4. Електронні файли видаляються з основних місць зберігання, а доступи до них припиняються.

16. Права осіб щодо їхніх даних

16.1. Особа має право, наскільки це передбачено законом і внутрішніми процедурами:

- знати, які її дані обробляються;
- отримати інформацію про мету обробки;
- виправити неточні дані;
- відкликати згоду, якщо обробка базується на згоді;
- вимагати обмеження обробки або видалення даних, якщо це можливо;
- поставити запитання або подати скаргу щодо обробки даних.

16.2. Канали повідомлення щодо захисту даних

16.2.1. Запити щодо персональних даних можуть подаватися на e-mail: i@mhc.center

16.2.2. Чутливі звернення щодо конфіденційності, PSEA, safeguarding або захисту дітей – на e-mail: safeguarding@mhc.center

17. Витік або порушення безпеки даних

17.1. Будь-яка особа, яка дізналася про можливий витік даних, втрату документів, несанкціонований доступ, помилкову передачу або інше порушення конфіденційності, повинна негайно повідомити відповідальну особу.

17.2. Прикладами порушення можуть бути:

- втрата паперових форм або списків;
- надсилання файлу не тому отримувачу;
- доступ сторонньої особи до бази даних;
- викрадення або втрата ноутбука чи телефону;
- публікація фото без згоди;
- розголошення деталей кейсу;
- пересилання чутливої інформації у незахищений чат;
- несанкціоноване копіювання даних.

17.3. Після повідомлення Організація:

- оцінює характер і масштаб порушення;
- вживає заходів для обмеження шкоди;
- визначає, чи потрібно повідомити постраждалих осіб, донора або компетентні органи;
- документує інцидент;
- вживає коригувальних заходів для запобігання повторенню.

18. Обов'язки працівників, волонтерів і консультантів

18.1. Усі особи, які мають доступ до даних, зобов'язані:

- дотримуватися цієї Політики;
- збирати лише необхідні дані;
- не розголошувати конфіденційну інформацію;
- захищати документи, пристрої та облікові записи;
- не передавати дані стороннім особам без підстав;
- повідомляти про витоки або ризики;
- видаляти або повертати дані після завершення співпраці;
- проходити інструктаж або навчання, якщо це передбачено Організацією.

18.2. Порушення конфіденційності може тягнути дисциплінарні заходи, розірвання договору, припинення співпраці або інші дії відповідно до внутрішніх політик і законодавства.

19. Навчання, впровадження та перегляд

19.1. Організація забезпечує:

- ознайомлення працівників, волонтерів, консультантів і партнерів із цією Політикою;
- включення положень щодо конфіденційності до договорів або інструктажів, де це доречно;
- періодичні нагадування щодо захисту даних;

- обмеження доступу до чутливої інформації;
- перегляд цієї Політики не рідше одного разу на рік або раніше у разі зміни законодавства, донорських вимог, операційного контексту або внутрішніх процедур.

20. Заключні положення

20.1. Ця Політика є обов'язковою для всіх осіб, на яких поширюється її дія.

20.2. Конфіденційність є ключовим принципом роботи Організації, особливо у сфері психічного здоров'я, психосоціальної підтримки, захисту дітей, PSEA та роботи з вразливими групами.

20.3. У разі сумнівів щодо обробки або передачі даних особа повинна звернутися до керівництва або уповноваженої особи до здійснення такої дії.

Галина Дмитренко,

В.О. голови ГО «Кризовий центр психічного здоров'я»

Halyna Dmytrenko,

Acting Head of NGO "Mental Health Crisis Center"