

«ЗАТВЕРДЖЕНО»
Протоколом засідання
Наглядової Ради
БО «БФ «АДРА УКРАЇНА»
від «___» червня 2025 р.
№ _____



Політика захисту даних
БО "БФ "АДРА Україна"

Київ -2025

Мета

Адвентистське агентство розвитку та допомоги в Україні (ADRA Ukraine) зобов'язується вести свою діяльність відповідно до всіх чинних законів і нормативних актів про захист персональних даних. Ця політика визначає очікувану поведінку працівників АДРА Україна та третіх осіб щодо збору, використання, зберігання, передачі, розкриття та знищення персональних даних.

Персональні дані - це будь-яка інформація (включаючи думки та наміри), що стосується ідентифікованої або ідентифікованої фізичної особи (Суб'єкта даних). На них поширюються певні правові гарантії та інші нормативні акти, які накладають обмеження на те, як організація може обробляти персональні дані.

Організація, яка обробляє персональні дані та приймає рішення щодо їх використання, називається Контролером даних. АДРА Україна, як Контролер даних, несе відповідальність за забезпечення дотримання вимог щодо захисту даних, викладених у цій політиці. Недотримання цих вимог може призвести до скарг, регуляторних дій, штрафів та/або шкоди репутації АДРА Україна. Керівництво АДРА Україна повністю віддане забезпеченню безперервного та ефективного впровадження цієї політики та очікує, що всі співробітники, партнери, волонтери, підрядники та інші треті сторони поділяють це зобов'язання.

Будь-яке порушення цієї політики буде розглядатися серйозно і може призвести до дисциплінарних або економічних санкцій. Ця політика була затверджена Наглядовою радою ADRA

Сфера застосування

Ця політика поширюється на АДРА Україна та всі місця, де організація обробляє персональні дані:

- У контексті функціонування та діяльності організації
- За надання або пропозицію товарів чи послуг
- З метою маркетингу та фандрейзингу

Якщо вимоги цієї політики суперечать вимогам національного законодавства, будь ласка, проконсультуйтеся з персоналом АДРА Україна з питань захисту даних, наприклад, з директором програми, спеціалістом із захисту даних, ІТ-спеціалістом, керівником юридичного відділу або координатором MEAL.

Визначення

Анонімізація

Дані, змінені таким чином, що жодна особа не може бути ідентифікована за цими даними (прямо чи опосередковано) жодним способом або жодною особою.

Згода

Будь-яке вільно надане, конкретне, усвідомлене та однозначне волевиявлення Суб'єкта даних, яким він шляхом заяви або чіткої ствердної дії надає згоду на обробку персональних даних, що стосуються його/її.

Витік даних

Порушення безпеки, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, що передаються, зберігаються або обробляються іншим чином.

Контролер даних

Фізична особа або організація, яка самостійно або спільно з іншими визначає цілі та засоби обробки персональних даних.

Обробник даних

Фізична особа або організація, яка обробляє персональні дані від імені контролера даних.

Захист даних

Процес захисту персональних даних від несанкціонованого або незаконного розкриття, доступу, зміни, перекручення, обробки, передачі чи знищення.

Суб'єкт даних

Будь-яка особа, 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 факторів, характерних для фізичної, фізіологічної, генетичної, психічної, економічної, культурної чи соціальної ідентичності цієї особи.

Шифрування

Процес перетворення інформації або даних у код, щоб запобігти несанкціонованому доступу.

Персональні дані

Будь-яка інформація (включаючи думки та наміри), що стосується ідентифікованої фізичної особи або особи, яку можна ідентифікувати.

Порушення персональних даних

Порушення безпеки, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або несанкціонованого доступу до персональних даних, що передаються, зберігаються або іншим чином обробляються.

Обробка

Будь-яка операція або сукупність операцій, що здійснюються над персональними даними чи наборами персональних даних, як автоматизовано, так і неавтоматизовано. Операції, що виконуються, можуть включати збір, запис, організацію, структурування, зберігання, резервне копіювання даних, адаптацію або зміну, пошук, консультацію, використання, розкриття шляхом передачі, розповсюдження або іншого надання, узгодження або комбінування, обмеження, видалення або знищення.

Процесор

Фізична або юридична особа, орган державної влади, агентство або інший орган, який обробляє персональні дані від імені контролера.

Профілювання

Будь-яка форма автоматизованої обробки персональних даних, коли персональні дані використовуються для оцінки конкретних або загальних характеристик, що стосуються суб'єкта даних. Зокрема, для аналізу або прогнозування певних аспектів, що стосуються продуктивності цієї особи на роботі, економічної ситуації, здоров'я, особистих уподобань, інтересів, надійності, поведінки, місцезнаходження або пересування.

Псевдонімізація

Дані, змінені таким чином, що жодна особа не може бути ідентифікована за цими даними (прямо чи опосередковано) без "ключа", який дозволяє повторно ідентифікувати дані.

Спеціальні категорії даних

Це стосується:

- персональні дані, що розкривають **расове або етнічне походження**;
- персональні дані, що розкривають **політичні погляди**;
- персональні дані, що розкривають **релігійні або філософські переконання**;
- персональні дані, що свідчать про **членство в профспілці**;
- **генетичні дані**;
- **біометричні дані** (якщо вони використовуються з метою ідентифікації);
- дані, що стосуються **здоров'я**;
- дані, що стосуються **сексуального життя** людини;
- дані про **сексуальну орієнтацію** особи.

Персонал

Особи, які працюють на умовах повної або часткової зайнятості в АДРА Україна за трудовим договором. Включає штатних працівників, тимчасових працівників та асоційованих осіб, а також незалежних підрядників та постачальників послуг, які можуть бути залучені до обробки персональних даних.

Третя сторона

Зовнішня організація, з якою АДРА Україна обмінюється персональними даними або яка обробляє дані від імені АДРА Україна.

Навчання та підвищення обізнаності

Наглядова рада АДРА повинна переконатися, що всі співробітники знають і дотримуються змісту цієї політики. Крім того, керівництво повинно забезпечити, щоб усі треті сторони, які займаються обробкою персональних даних від імені АДРА (тобто їхні Обробники даних), знали та дотримувалися змісту цієї політики.

Запевнення у дотриманні таких вимог повинні бути отримані від усіх третіх осіб, як організацій, так і фізичних осіб, перед наданням їм доступу до персональних даних, які контролюються АДРА Україна.

Захист даних за задумом

Щоб гарантувати, що всі вимоги щодо захисту даних визначені та враховані при розробці нових систем або процесів та/або при перегляді чи розширенні існуючих систем або процесів, кожна нова система або процес повинні пройти процес затвердження перед продовженням роботи.

Моніторинг відповідності

Співробітники відділу захисту даних розроблять план з графіком виправлення будь-яких виявлених недоліків у визначені та розумні строки. Про будь-які виявлені серйозні недоліки буде повідомлено вищому керівництву АДРА Україна, яке здійснюватиме моніторинг.

Принципи захисту даних

АДРА Україна вимагає від усіх співробітників і третіх сторін дотримуватися відповідних національних законів щодо наступних принципів захисту даних, які регулюють використання персональних даних, для яких АДРА Україна є контролером даних.

- **Принцип 1: Персональні дані повинні оброблятися законним, справедливим і прозорим чином по відношенню до суб'єкта даних.** Це означає, що АДРА Україна повинна повідомити суб'єкта даних про те, яка обробка буде відбуватися (прозорість), обробка повинна відповідати опису, наданому суб'єкту даних (справедливість), і вона повинна здійснюватися для однієї з цілей, визначених у відповідному нормативному акті про захист даних (законність).
- **Принцип 2: Персональні дані повинні збиратися для визначених, чітких і законних цілей і не повинні надалі оброблятися у спосіб, несумісний з цими цілями.** Це означає, що АДРА Україна повинна точно визначити, для чого будуть використовуватися зібрані персональні дані, і обмежити обробку цих персональних даних лише тим, що необхідно для досягнення зазначеної мети.
- **Принцип 3: Персональні дані повинні бути адекватними, релевантними та обмежуватися лише тим, що необхідно для цілей, для яких вони обробляються.** Це означає, що АДРА Україна не повинна зберігати будь-які персональні дані понад те, що є необхідним.
- **Принцип 4: Персональні дані повинні бути точними та постійно оновлюватися.** Це означає, що АДРА Україна повинна мати процедури для виявлення та усунення застарілих, невірних та надлишкових персональних даних.
- **Принцип 5: Персональні дані повинні зберігатися у формі, яка дозволяє ідентифікувати суб'єкта даних, не довше, ніж це необхідно для цілей, для яких обробляються персональні дані.** Це означає, що АДРА Україна повинна, де це можливо, зберігати персональні дані таким чином, щоб обмежити або унеможливити ідентифікацію

суб'єкта даних.

- **Принцип 6: Персональні дані повинні оброблятися у спосіб, що забезпечує належну безпеку персональних даних, включаючи захист від несанкціонованої або незаконної обробки, а також від випадкової втрати, знищення або пошкодження.** Це означає, що АДРА Україна повинна використовувати відповідні технічні та організаційні заходи для забезпечення постійного збереження цілісності та конфіденційності Персональних даних.
- **Принцип підзвітності: Контролер даних повинен нести відповідальність і бути здатним продемонструвати дотримання вимог.** Це означає, що АДРА Україна повинна продемонструвати, що шість принципів захисту даних (описаних вище) дотримуються для всіх персональних даних, за які вона несе відповідальність.

Збір даних

Джерела даних

Персональні дані можуть збиратися тільки від самого суб'єкта даних, якщо тільки не застосовується одна з наступних умов:

- Характер ділової мети обумовлює необхідність збору персональних даних від інших осіб або органів.
- Збір повинен здійснюватися за надзвичайних обставин з метою захисту життєво важливих інтересів Суб'єкта даних або запобігання серйозним втратам чи травмам іншої особи.
- Якщо персональні дані збираються не від Суб'єкта даних, а від когось іншого, Суб'єкт даних повинен бути поінформований про збір даних, за винятком випадків, коли застосовується один з наступних пунктів:
- Суб'єкт даних отримав необхідну інформацію іншими способами. Наприклад, він вже був поінформований Третьою особою про те, що його дані будуть передані АДРА Україна.
- Інформація повинна залишатися конфіденційною у зв'язку із зобов'язанням зберігати професійну таємницю

Якщо було визначено, що повідомлення Суб'єкта даних є необхідним, повідомлення повинно відбутися негайно, але в жодному разі не пізніше, ніж:

- Один календарний місяць з моменту першого збору або запису персональних даних
- Під час першої комунікації, якщо використовується для зв'язку з Суб'єктом даних
- У момент розкриття інформації, якщо вона була розкрита іншому одержувачу

Законні підстави для використання та обробки даних

АДРА Україна використовує персональні дані для наступних широких цілей:

- Загальне управління та адміністрування АДРА Україна
- Надання послуг донорам та бенефіціарам АДРА Україна

- Поточне адміністрування та управління донорськими послугами.
- Постійне управління волонтерами, адвокатами та прихильниками
- Для підзвітності перед спонсорами та донорами

Використання інформації Суб'єкта даних завжди має розглядатися з його точки зору, а також з точки зору того, чи буде таке використання відповідати його очікуванням, або ж він може висловити заперечення.

АДРА Україна обробляє персональні дані відповідно до всіх чинних законів та застосовних договірних зобов'язань. Зокрема, АДРА Україна не оброблятиме жодних персональних даних, якщо не буде дотримано принаймні однієї з наступних вимог:

- Обробка необхідна для виконання договору, стороною якого є суб'єкт даних, або для того, щоб вжити заходів на прохання суб'єкта даних до укладення договору.
- Обробка необхідна для дотримання юридичного зобов'язання, яке має контролер даних
- Обробка необхідна для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи
- Обробка необхідна для виконання завдання, що здійснюється в інтересах суспільства або при здійсненні офіційних повноважень, покладених на контролера даних
- Обробка необхідна для цілей законних інтересів, переслідуваних контролером даних або третьою стороною (за винятком випадків, коли такі інтереси переважають інтереси або основоположні права і свободи суб'єкта даних, зокрема, коли суб'єкт даних є дитиною)
- Суб'єкт даних надав згоду на обробку своїх персональних даних для однієї або декількох конкретних цілей

Згода буде отримана лише тоді, коли жодна з інших законних підстав для обробки не застосовується.

Отримання згоди

Персональні дані повинні бути отримані тільки законними і справедливими способами і, де це необхідно, з відома і згоди відповідної особи.

Під час отримання згоди АДРА Україна забезпечить наявність наступних умов:

- Переконайтеся, що запит на отримання згоди подається таким чином, щоб його можна було чітко відрізнити від будь-яких інших питань, у зрозумілій і легкодоступній формі та з використанням чіткої і простої мови.
- Переконайтеся, що згода надається вільно (тобто не ґрунтується на договорі, умовою якого є обробка персональних даних, які не є необхідними для виконання цього договору).
- Задokumentуйте дату, спосіб і зміст розкриття інформації, а також термін дії, обсяг і волевиявлення наданих згод.
- Надавати суб'єкту даних можливість відкликати свою згоду в будь-який час, гарантуючи, що відкликати згоду буде так само легко, як і надати її в першу чергу

Суб'єктам даних має бути надана інформація про мету обробки їхніх персональних даних на етапі збору інформації.

Обробка даних за будь-яких обставин, коли Згода не була отримана на конкретну обробку, про яку йдеться

Окрім забезпечення законних підстав для нової обробки будь-яких даних, АДРА Україна розгляне наступні додаткові умови для визначення справедливості та прозорості будь-якої обробки, що виходить за рамки первісної мети, для якої були зібрані персональні дані:

- Будь-який зв'язок між метою, для якої були зібрані персональні дані, і причинами передбачуваної подальшої обробки.
- Контекст, в якому були зібрані персональні дані, зокрема щодо відносин між суб'єктом даних та контролером даних.
- Характер персональних даних, зокрема, чи обробляються спеціальні категорії даних, чи обробляються персональні дані, пов'язані з кримінальними судимостями та правопорушеннями.
- Можливі наслідки запланованої подальшої обробки для суб'єкта даних.
- Існування відповідних гарантій щодо подальшої обробки, які можуть включати шифрування, анонімізацію або псевдонімізацію.

Спеціальні категорії даних

АДРА Україна обробляє особливі категорії даних (також відомі як конфіденційні дані) лише тоді, коли Суб'єкт даних надає явну згоду на таку обробку або коли застосовується одна з наступних умов:

- Обробка стосується персональних даних, які вже були оприлюднені суб'єктом даних
- Обробка необхідна для встановлення, здійснення або захисту правових вимог
- Обробка є спеціально дозволеною або вимагається законом, включаючи зобов'язання, що впливають з угод з державними установами.
- Обробка необхідна для захисту життєво важливих інтересів Суб'єкта даних або іншої фізичної особи, якщо Суб'єкт даних фізично або юридично не здатний дати згоду.
- Інші умови, в тому числі обмеження, засновані на національному законодавстві, пов'язані з обробкою генетичних даних, біометричних даних або даних, що стосуються здоров'я

Якщо обробляються особливі категорії даних, АДРА Україна вживатиме додаткових заходів захисту.

Дані про дітей

Діти, які не досягли 18 років, не можуть надавати згоду на обробку персональних даних особисто. Згода має бути отримана від особи, яка несе батьківську відповідальність за дитину

(мати, батько, опікун тощо).

Якщо АДРА Україна вимагає згоди батьків на обробку персональних даних, запропонованих безпосередньо дитині, перед обробкою персональних даних дитини необхідно отримати інструкції та схвалення від співробітників відділу захисту даних.

Якість даних

АДРА Україна вживає всіх необхідних заходів для забезпечення того, щоб персональні дані, які вона збирає та обробляє, були повними та точними, а також оновлювалися для відображення поточної ситуації Суб'єкта даних. АДРА Україна вживає таких заходів для забезпечення якості даних

- виправлення персональних даних, про які відомо, що вони є неправильними, неточними, неповними, двозначними, такими, що вводять в оману, або застарілими, навіть якщо суб'єкт даних не вимагає їх виправлення
 - зберігання персональних даних лише протягом періоду, необхідного для задоволення дозволеного використання або застосовного законодавчо встановленого терміну зберігання
 - видалення персональних даних у разі порушення будь-якого з принципів захисту даних або якщо персональні дані більше не потрібні.
 - обмеження, а не видалення персональних даних, наскільки це можливо:
 - Закон забороняє стирання.
 - Видалення порушить законні інтереси суб'єкта даних.
 - Суб'єкт даних заперечує, що його персональні дані є правильними, і неможливо чітко встановити, чи є його інформація правильною чи неправильною.
-

Профілювання та автоматизоване прийняття рішень

АДРА Україна використовуватиме профілювання та автоматизоване прийняття рішень лише тоді, коли це необхідно для укладення або виконання договору з Суб'єктом даних або коли це дозволено законом. Якщо АДРА Україна використовує профілювання та автоматизоване прийняття рішень, Суб'єкту даних буде надана можливість заперечити проти цього.

АДРА Україна також повинна гарантувати, що все профілювання та автоматизоване прийняття рішень щодо Суб'єкта даних ґрунтується на точних даних.

Зберігання даних

Щоб забезпечити справедливу обробку, АДРА Україна не зберігатиме персональні дані довше, ніж це необхідно для цілей, для яких вони були спочатку зібрані, або для подальшої обробки, а також відповідно до національного та/або місцевого законодавства.

Усі персональні дані повинні бути видалені або знищені якомога швидше, якщо підтверджено, що в їх збереженні більше немає потреби.

Захист даних

АДРА Україна вживатиме фізичних, технічних та організаційних заходів для забезпечення безпеки персональних даних. Це включає запобігання втраті або пошкодженню, несанкціонованій зміні, доступу або обробці, а також іншим ризикам, яким вони можуть піддаватися внаслідок дій людини або фізичного чи природного середовища.

Нижче наведено стислий опис заходів безпеки, пов'язаних із персональними даними:

- Запобігати доступу сторонніх осіб до систем обробки даних, в яких обробляються персональні дані.
- Заборонити особам, які мають право використовувати систему обробки даних, доступ до персональних даних, що виходить за межі їхніх потреб та повноважень.
- Переконайтеся, що персональні дані в процесі електронної передачі під час транспортування не можуть бути прочитані, скопійовані, змінені або видалені без дозволу.
- Забезпечити наявність журналів доступу для встановлення того, чи були персональні дані введені в систему обробки даних, змінені в ній або видалені з неї, і якщо так, то ким саме.
- Переконайтеся, що у випадку, коли обробка здійснюється процесором даних, дані можуть оброблятися тільки відповідно до інструкцій контролера даних.
- Переконайтеся, що персональні дані захищені від небажаного знищення або втрати.
- Переконайтеся, що персональні дані, зібрані для різних цілей, можуть оброблятися окремо.
- Переконайтеся, що персональні дані не зберігаються довше, ніж це необхідно.

Запити правоохоронних органів та розкриття інформації

За певних обставин дозволяється розкривати персональні дані без відома або згоди суб'єкта даних.

Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи допускається у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту, прав людини та з метою проведення

Всеукраїнського перепису населення.

Тренінг із захисту даних

Усі співробітники АДРА Україна мають свої обов'язки відповідно до цієї політики, про які їм розповідають під час вступного інструктажу. Крім того, регулярні тренінги та інформування щодо захисту даних проводяться за допомогою онлайн-тренінгів та інших засобів комунікації для всіх співробітників.

Навчання та інструктаж складаються, як мінімум, з таких елементів:

- Принципи захисту даних.
- Обов'язок кожного використовувати та дозволяти використання персональних даних лише уповноваженим особам і для уповноважених цілей.
- Необхідність і належне використання форм і процедур, прийнятих для реалізації цієї політики
- Правильне використання паролів, токенів безпеки та інших механізмів доступу.
- Важливість обмеження доступу до персональних даних, наприклад, за допомогою захищених паролем екранних заставок і виходу з системи, коли в ній не працює уповноважена особа.
- Надійне зберігання ручних файлів, роздруківок та електронних носіїв інформації.
- Необхідність отримання відповідного дозволу та використання належних засобів захисту для всіх випадків передачі персональних даних за межі внутрішньої мережі та фізичних офісних приміщень.
- Належна утилізація персональних даних шляхом використання безпечних засобів знищення.
- Будь-які особливі ризики, пов'язані з конкретною діяльністю або обов'язками відділу.

Перекази третім особам

АДРА Україна передаватиме персональні дані або надаватиме доступ до них третім особам лише тоді, коли буде впевнена, що інформація буде оброблена на законних підставах та належним чином захищена одержувачем.

Якщо обробка здійснюється третьою стороною, АДРА Україна спочатку визначить, чи вважається ця третя сторона відповідно до чинного законодавства Контролером даних або Обробником даних, що передаються, відповідно до чинного законодавства.

Якщо третя сторона вважається Контролером даних, АДРА Україна укладе відповідну угоду з Контролером для уточнення обов'язків кожної сторони щодо переданих персональних даних. Дані можуть передаватися на основі даних про чутливість класифікації та інформації АДРА Україна.

Якщо третя сторона вважається Обробником даних, АДРА Україна укладе з ним відповідну угоду про обробку даних. Угода повинна вимагати від Обробника даних захищати персональні дані від подальшого розголошення та обробляти персональні дані лише відповідно до інструкцій АДРА Україна. Крім того, угода вимагатиме від Обробника даних вжиття відповідних технічних та організаційних заходів для захисту персональних даних, а

також процедур надання
повідомлень про порушення персональних даних.

Коли АДРА Україна передає послуги на аутсорсинг третій стороні, вона визначає, чи буде ця третя сторона обробляти персональні дані від її імені, і чи буде цей аутсорсинг передбачати передачу персональних даних третім особам. У будь-якому випадку, АДРА Україна подбає про те, щоб включити в договір про аутсорсинг відповідні положення про таку обробку та передачу третім особам.

У разі необхідності АДРА Україна залишає за собою право проводити аудит обробки персональних даних, що здійснюється третіми сторонами, особливо щодо технічних та організаційних заходів, які вони застосовують.

Разом із Угодою про обмін даних або як її складову, ADRA Ukraine підтримує протокол обміну даними, який регулює безпечне, відповідальне та обмежене розкриття даних бенефіціарів. Дані можуть передаватися лише у випадках, коли це прямо необхідно для моніторингу, оцінки проєкту або звітності перед донорами, і тільки за наявності формально затвердженої письмової угоди, підписаної сторонами, уповноваженими здійснювати такий моніторинг і оцінку. Персональні дані повинні бути анонімізовані, де це можливо. Якщо використання прямих ідентифікаторів (таких як імена або номери телефонів) є необхідним, дані мають передаватися у зашифрованому вигляді та лише уповноваженому персоналу, зазначеному в угоді. Сторона, що отримує дані, зобов'язана видалити їх не пізніше ніж через 30 днів після завершення передбаченого використання. Дані не можуть передаватися третім сторонам, не зазначеним в Угоді про обмін даними, включно з державними органами, якщо лише це не передбачено обов'язковою юридичною угодою. Усі сторони, які беруть участь в обміні даними, повинні забезпечувати сувору конфіденційність, використовувати захист паролем і негайно повідомляти про будь-які підозри щодо неправильного використання даних. Протокол обміну даними регулярно переглядається та оновлюється відповідно до найкращих практик і правових вимог у сфері захисту даних.

Скарги

Розгляд скарг на обробку персональних даних має здійснюватися відповідно до Політики АДРА Україна щодо механізму розгляду скарг та зворотного зв'язку (МЗЗ) та Стратегії захисту персональних даних АДРА Україна. Розслідування скарги буде проводитися в тому обсязі, який є доцільним, виходячи з суті конкретного випадку. Відповідальний персонал із захисту даних інформуватиме Суб'єкта даних про хід та результати розгляду скарги протягом розумного періоду часу.

Дані моніторингу після розподілу допомоги (PDM)

Дані моніторингу після розподілу допомоги (PDM), які збирає ADRA Ukraine, підлягають тим самим стандартам захисту даних, що зазначені в Політиці захисту даних, як і всі інші дані бенефіціарів. Дані PDM, які можуть включати відповіді на опитування, зворотний зв'язок та демографічну інформацію, збираються з метою оцінки ефективності,

релевантності та підзвітності наданої гуманітарної допомоги. Персональні ідентифікатори збираються лише за необхідності та повинні зберігатися в захищених зашифрованих системах. Усі дані PDM мають бути анонімізовані на якнайранішому етапі, щоб мінімізувати ризики для суб'єктів даних. Доступ до необроблених даних PDM обмежений уповноваженим персоналом MEAL та партнерами, які формально залучені до процесу моніторингу. Дані PDM зберігаються лише на період, необхідний для аналізу, звітності та аудиту, після чого мають бути видалені або анонімізовані згідно з графіком зберігання даних. Результати, отримані в рамках діяльності PDM, не повинні містити персонально ідентифіковану інформацію та мають поширюватися виключно в анонімізованій формі.

У випадку втручання у сфері психічного здоров'я та психосоціальної підтримки (MHPSS) проведення стандартного PDM може бути недоцільним через високий рівень чутливості відповідних даних. Такі заходи часто стосуються особистих, психологічних або травматичних переживань, що потребують підвищеного рівня конфіденційності та захисту. Тому можуть застосовуватись альтернативні методи моніторингу, які не ставлять під загрозу приватність або емоційне благополуччя бенефіціарів, відповідно до глобальних стандартів MHPSS та стандартів безпеки. Одним із практичних та етично виправданих способів збору зворотного зв'язку від бенефіціарів MHPSS є анонімні форми зворотного зв'язку, які не містять персонально ідентифікованої інформації та включають лише нечутливі демографічні дані, такі як вік і стать. Такий підхід дозволяє отримати змістовний зворотний зв'язок, одночасно зберігаючи гідність, приватність і психологічну безпеку бенефіціарів MHPSS.

Повідомлення про порушення

Будь-яка особа, яка підозрює, що сталося Порушення персональних даних через крадіжку або розголошення персональних даних, повинна негайно повідомити про це, надавши опис того, що сталося.

АДРА Україна розслідує всі повідомлені інциденти, щоб підтвердити, чи мало місце порушення персональних даних. Якщо факт порушення персональних даних підтверджено, АДРА Україна визначить критичність та кількість відповідних персональних даних. У разі порушення персональних даних, яке може завдати потенційної шкоди окремим особам, співробітники відділу захисту даних ініціюватимуть, координуватимуть та керуватимуть заходами реагування на порушення персональних даних.

Публікація

Ця політика є доступною для всіх співробітників та партнерів АДРА Україна. Просимо всіх співробітників та асоційованих осіб поставити свій підпис на підтвердження того, що вони прочитали та зрозуміли цю політику.