Використання "конфіденційних" даних

Посібник з обробки конфіденційних даних

Зміст

Обґрунтування	1
Область застосування даних	1
Що таке конфіденційні дані та чому вони відрізняються від інших типів персональних даних?	2
Визначення ключових термінів	2
Планування	5
Планування збору даних	7
Збір даних	8
Зберігання даних	8
Аналіз даних	8
Передача даних донору, партнеру або іншій третій стороні (за необхідності)	9
Поширені запитання	9
Супутні документи:	11

Обґрунтування

Для більшості програм та інших видів діяльності Mercy Corps збирають певну особисту інформацію про осіб, яких ми обслуговуємо та з якими працюємо, для багатьох також збирають інформацію про , яка класифікується як конфіденційна. Збір конфіденційних даних необхідний нам для виконання нашої роботи та обслуговування учасників програми та їх спільнот, в яких ми працюємо. Тому, оскільки ми збираємо та використовуємо конфіденційні дані, життєво важливо вжити всіх необхідних заходів для забезпечення захисту цих даних. Нездатність захистити конфіденційні дані може призвести до серйозних збитків для суб'єкта даних, у тому числіу тому числі, до дискримінації та загрози безпеці.

Область застосування даних

Цей посібник поширюється на всю обробку конфіденційних даних у межах всього агентства. Він застосовується до конфіденційних даних, зібраних у програмних та операційних цілях, а також у будь-якій іншій ситуації, де є конфіденційні дані. У цьому документі описані необхідні кроки при обробці конфіденційних даних.

Що таке конфіденційні дані та чому вони відрізняються від інших типів персональних даних?

Конфіденційні дані – це зазвичай такі дані, як культурний профіль людини, її сексуальна орієнтація, біометричні та генетичні дані про стан здоров'я. Це дані, які у разі розкриття, доступу або розповсюдження неналежним чином можуть призвести до:

- заподіяння шкоди (наприклад, санкцій, дискримінації та загрози безпеці) будь-якій особі, у тому числіу тому числі для джерела інформації або інших осіб або груп, що ідентифікуються;
- негативного впливу на здатність організації здійснювати свою діяльність чи громадське сприйняття цієї організації.

Приклад 1:

Програма реалізується в одній із спільнот, і в ході проекту кілька учасників дізнаються, що вони ВІЛ-інфіковані. Ця інформація випадково передається старшим членам спільноти, внаслідок чого учасникам програми може бути заподіяна значна шкода і навіть фізична загроза.

Приклад 2:

Офіс планує святкування та збирає інформацію про дієтичні вимоги членів команди. Декілька членів команди вказали, що їм потрібна кошерна або халяльна їжа. Електронна таблиця, де зазначено, хто з членів команди має особливі дієтичні вимоги, передається всій команді. Деякі члени команди не розповіли про свою релігію, оскільки побоюються дискримінації.

До конфіденційних даних необхідно ставитися з більшою обережністю, оскільки їх збір та використання з більшою ймовірністю може порушити основні права або свободи людини або завдати значної шкоди, у тому числі призвести до дискримінації або фізичної небезпеки, якщо вони будуть використані не за призначенням.

Загальне положення про захист даних (GDPR) визначає ряд типів даних, які відносяться до спеціальної категорії конфіденційних даних, та детально описує конкретні умови обробки цих типів даних. Однак важливо відзначити, що в деяких контекстах дані, які не входять до стандартної спеціальної категорії конфіденційних даних, все одно можуть бути конфіденційними в силу конкретного контексту. Для цілей цього посібника ці типи даних будуть називатися контекстуально-конфіденційними даними.

Даний посібник розроблено як додаток до Політики відповідального використання даних Mercy Corps, а також Політики управління програмами (яка також включає Політику MELагентства) і застосовується до збору конфіденційних даних у всіх контекстах, у тому числі, але не виключно, дані штаб-квартири, програм та MEL.

Визначення ключових термінів

- **Оперативні дані Mercy Corps** - будь-яка одиниця інформації, що складається з літер, цифр, символів, зображень, відео- та голосових записів, геопросторових координат або ідентифікаторів розташування, картографічних даних або будь-якої їх комбінації, що

обробляються Mercy Corps. Це може включати, але не обмежуватися даними про членів команди Mercy Corps, постачальників, донорів або партнерів. Дані існують як у цифровій, так і у фізичній формі.

- **Конфіденційні дані-**Ця інформація часто використовуються як основа для цілеспрямованого впливу на певну групу або окрему особу. Звичайними прикладами є раса, релігія, політичні погляди, сексуальна орієнтація, здоров'я чи біометрична інформація.

  В рамках цієї примітки до конфіденційних даних відносяться "конфіденційні дані спеціальної категорії", як зазначено в GDPR, та "конфіденційні дані контекстуального характеру".

- **Конфіденційні дані спеціальної категорії-** GDPR встановлює особливі вимоги до обробки всіх конфіденційних даних спеціальної категорії, яких має бути дотримано. GDPR визначає конфіденційні дані спеціальної категорії як:

  - персональні дані, що розкривають расове чи етнічне походження;
  - особисті дані, що розкривають політичні погляди;
  - персональні дані, що розкривають релігійні чи філософські переконання;
  - персональні дані, які розкривають членство у профспілці;
  - генетичні дані;
  - біометричні дані (якщо вони використовуються з метою ідентифікації);
  - дані щодо здоров'я;
  - дані щодо сексуального життя людини; і
  - дані щодо сексуальної орієнтації людини

- **Контекстуально-конфіденційні дані** - дані, які не підпадають під категорії конфіденційних даних, визначених GDPR, але які в силу контексту, в якому вони обробляються, є конфіденційними за своєю природою і можуть завдати значної шкоди суб'єкту даних у разі розкриття.

- **Порушення персональних даних** - Порушення персональних даних можна загалом визначити як інцидент безпеки, який вплинув на конфіденційність, цілісність чи доступність персональних даних. Коротко кажучи, порушення персональних даних матиме місце щоразу, коли будь-які персональні дані будуть втрачені, знищені, пошкоджені або розкриті; якщо хтось отримає доступ до даних або передасть їх без належного дозволу; або якщо дані стануть недоступними, наприклад, коли вони будуть зашифровані шкідливою програмою з вимогою викупу або випадково втрачені чи знищені.

- **Програмні дані** - будь-яка одиниця інформації, що складається з літер, цифр, символів, зображень, відео- та голосових записів або будь-якої їх комбінації, що відноситься до

учасників програми, її реалізації та результатів. Дані існують як у цифровій, так і у фізичній формі.

- **Політика відповідального використання даних Mercy Corps** – політика агентства, спрямована на встановлення принципів прозорого, безпечного та відповідального використання персональних даних у рамках агентства та впровадження цих принципів у нашу повсякденну роботу.

- **Інформована згода** - процес отримання добровільного дозволу на збір даних будь-якого роду, заснований на чіткому усвідомленні та розумінні учасниками фактів, результатів та наслідків будь-якої участі. Ця згода може бути надана як у письмовій, так і в усній заяві або шляхом чіткої ствердної дії. Згода повинна бути отримана в момент збору Персональних даних або якнайшвидше після цього.

- **Явна згода** - Явна згода вимагає дуже чіткої та конкретної заяви про згоду. Необхідно вести облік того, коли і як була отримана згода, і що саме було сказано суб'єктам даних при отриманні згоди. У явній згоді має бути зазначений характер даних спеціальної категорії; і вона має бути окремою від будь-яких інших згод, які ви запитуєте.

- **Деідентифікація** - будь-які дії або методи обробки даних, спрямовані на запобігання прямому та/або непрямому розкриттю особи учасника або іншої особи. Типи прикладів: Анонімізація (тобто видалення певних обсягів персональних даних або застосування діапазону значень до певних наборів персональних даних) та псевдонімізація (тобто обробка персональних даних таким чином, що персональні дані більше не можуть бути віднесені до конкретного суб'єкта даних або сім'ї суб'єктів даних) без використання додаткової інформації, такої, як унікальні ідентифікатори або хеші).

- **Персонально ідентифікована інформація (PII)** - Інформація, що відноситься до ідентифікованої або тієї, що підлягає ідентифікації фізичною особою ("Суб'єкт даних"); ідентифікована особа - це особа, яка може бути прямо або опосередковано ідентифікована, зокрема, за ідентифікаційним номером або за одним чи декількома факторами, характерними для її фізичної, фізіологічної, психічної, економічної, культурної або соціальної ідентичності. Це тісно пов'язане з **демографічно ідентифікованою інформацією (DII)**, яка може бути використана для ідентифікації спільноти або окремої групи, чи то географічної, етнічної, релігійної, економічної чи політичної.

- **Безпечне зберігання** – доступ до даних мають лише окремі співробітники Mercy Corps; вживають заходів для запобігання крадіжці та неправильному використанню даних. Безпечне зберігання – доступ до даних мають лише визначені співробітники Mercy Corps; вживають заходів для запобігання крадіжці та неправильному використанню даних. Файл зберігається надійно, якщо:
  - Він зберігається на платформі, яка має/відповідає високим стандартам безпеки, захисту даних та конфіденційності
  - Доступ обмежений лише для необхідних сторін
  - Доступ регулярно переглядається та коригується за необхідності

- Додаткові вимоги встановлені для програм Mercy Corps у нещодавно прийнятій Політиці MEL, зокрема, Стандарт 9 вимагає, щоб усі програми забезпечували безпеку роботи з даними, відповідно до Політики відповідального використання даних, та з вимогами донорів.

- **Визначені члени команди Mercy Corps** - члени команди, яким необхідний доступ до ідентифікованої інформації для виконання завдань, характерних для їхньої роботи, таких як задоволення потреб учасників програми та завершення програмних заходів.

- **Суб'єкт даних** - будь-яка фізична особа, від імені якої та про яку збирають дані прямо, опосередковано або через третю сторону, і яка може бути ідентифікована прямо або опосередковано, зокрема шляхом посилання на Персональні дані.

- **Захист даних** - захист та запобігання несанкціонованому доступу, використанню або розповсюдженню персонально ідентифікованої інформації (PII), демографічно ідентифікованої інформації (DII) та інших конфіденційних даних про людину або групу протягом циклу даних управління програмою або проектом, а також після завершення програми або проекту. У Політиці відповідального використання даних Mercy Corps викладено вимоги захисту даних, і агентство також підпорядковується іншим правовим/регулятивним рамкам, таким як Загальне положення про захист даних Європейського Союзу (GDPR).

Додаткові визначення, пов'язані з відповідальними даними, див. у документі "Визначення відповідальних даних".

Планування

- Розгляньте, які типи даних будуть зібрані і задокументуйте це на етапі планування проекту, в Оцінці впливу на конфіденційність (PIA).

- Якщо план передбачає збирання та/або документування та/або зберігання будь-яких конфіденційних даних, особливу увагу слід приділити тому, як і чому ці дані використовуються. Подумайте, чи необхідний збір цих даних для досягнення необхідних результатів програми або проекту, чи достатньо альтернативного типу даних. Збирати конфіденційні дані слід лише у разі потреби. Зверніть увагу, що збір конфіденційних даних, за умови правильного підходу, є дорогим процесом. Знімаючи тягар непотрібного збору даних, ви дозволяєте командам заощадити час і ресурси для іншої необхідної роботи. Якщо ви визначили, що PII потрібна, не застосовуйте короткі шляхи. Якщо ваших ресурсів, виділених на збирання та керування конфіденційними даними, недостатньо для того, щоб робити це добре, будь ласка, переосмисліть всі ризики, на які ви можете наражати спільноти, з якими ви працюєте.

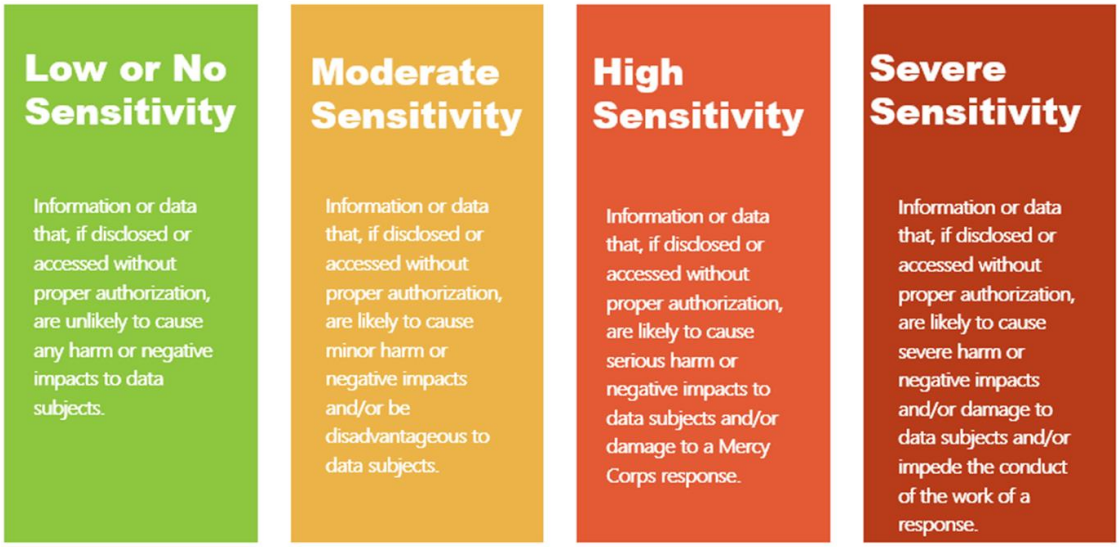
- Подумайте, які технології будуть використовуватися для збору та зберігання інформації. Застосовувані технологіїповинні включати відповідні гарантії збору конфіденційної інформації.

- Як правило, чим конфіденційніші дані, тим більше запобіжних заходів необхідно передбачити. Конфіденційні дані зазвичай мають "високий" або "серйозний" рівень конфіденційності (див. малюнок 1). Крім того, чим більше наборів даних збирається, тим вищий ризик і тим більше має бути запобіжних засобів. Приклади запобіжних заходів включають, але не обмежуються цим:

    - Шифрування
    - Псевдонімізація
    - Дисоціація
    - Зберігання паперових файлів у закритих шафах з обмеженим доступом
    - Зберігання файлів на серверах Mercy Corps із рівнями захисту
    - Обмеження доступу до пристроїв Mercy Corps і лише для тих, хто повинен мати доступ для виконання своїх посадових обов'язків
    - Забезпечення блокування таких пристроїв, як ноутбуки, коли вони не використовуються
    - Рандомізація або агрегування точки GPS для просторових даних

- Чітко визначте, яку правову основу для обробки конфіденційних даних ви використовуватимете, і плануйте відповідним чином.
- Вимоги до звітності у грантових угодах повинні відповідати принципам "Не зашкодь" (наприклад, програма не повинна збирати інформацію, яка може поставити під загрозу безпеку учасників) та чітко описувати зобов'язання та угоди щодо платформ обміну даними, процеси з донором, партнерами та іншими зацікавленими сторонами, у тому числі вимоги щодо деідентифікації та анонімізації.
- Протокол безпеки даних на рівні програми є частиною Технологічного плану MEL (Стандарт 6) та описує міркування щодо даних членів команди, у тому числі рівні дозволів та протоколи для членів команди MC та не-MC.
- Якщо збір конфіденційних даних здійснюється в оперативних цілях Mercy Corps, сплануйте та викладіть міркування щодо даних, у тому числі щодо рівнів дозволів та протоколів.
- Подумайте та обґрунтуйте, як довго вам потрібно зберігати дані (термін зберігання). Це залежить від причин збору даних, вимог законодавства, вимог донорів та політики зберігання записів програми MC.
- Забезпечте наявність процесу знищення даних після закінчення терміну зберігання.

Малюнок 1:



Планування збору даних

- Оцінка впливу на конфіденційність проводиться для виявлення та управління ризиками конфіденційності даних, пов'язаними з будь-якою новою діяльністю, такою як нові програми, технології чи політики. Якщо передбачається збір конфіденційних даних, їх слід розглянути компетентною особою. Це може бути команда захисту даних та конфіденційності, ваш DPO або відповідно до політики MEL (Мінімальний стандарт № 9 - Конфіденційність та безпека даних):
    - Підзвітні - Директор по країні, або Директор з програм та менеджер програм, або начальник відділу
    - Відповідальна сторона, що рекомендується - Керівник програми MEL/Управління знаннями

- Завершіть оцінку конфіденційної інформації (Sensitive Information Assessment, SIA), пов'язану з PIA. У ній повинні бути задокументовані всі додаткові заходи захисту, які застосовуються для конфіденційних даних.

- Якщо в якості правової основи використовується згода, інформована згода вимагає, щоб суб'єкти даних були поінформовані про наступні пункти простими словами:

    - Які дані збираються, і навіщо вони потрібні

    - Кому буде надана інформація, у тому числі будь-яких зовнішніх партнерів та донорів

    - Чи здійснюватиметься міжнародний обмін даними

    - Як довго зберігатимуться дані

- Слід вести облік того, коли та як було отримано згоду та що було сказано суб'єкту даних. На етапі планування слід враховувати зразок того, що буде сказано суб'єктам даних для отримання згоди.

Збір даних

- Для кожного випадку збору даних існує протокол збору даних, який включає:
    - Додаткові заходи захисту конфіденційних даних
    - Задокументовані інструкції зі збору, очищення даних, перевірки та деідентифікації, якщо це застосовується.
    - Інструкції з можливих порушень безпеки даних для всіх зібраних кількісних та якісних даних (наприклад, втрачені або викрадені пристрої, зламані логіни тощо)
    - Інструкції з використання та захисту друкованих форм під час збору матеріалу
    - Вибіркові перевірки та моніторинг того, наскільки дотримано протоколів з охорони та захисту даних особою/особами, які здійснюють збір даних
- Все вищезазначене має бути пов'язане з SIA

Зберігання даних

- Доступ до файлів, що містять конфіденційну інформацію, повинен бути обмежений членам команди, яким необхідний доступ до цієї інформації для виконання необхідних робіт;систематична деідентифікація конфіденційної інформації проводиться перед зв'язуванням з TolaData або передачею третій стороні залежно від ситуації. Стандарт 8 політики MEL надає додаткові рекомендації з найкращої практики надання та зберігання даних MEL
- Дані зберігаються у місці, яке узгоджено за всіма відповідними політиками Mercy Corps (наприклад, Політика відповідального використання даних, Прийнятне використання).
- Конфіденційні дані повинні зберігатися не довше, ніж це необхідно. Після закінчення терміну зберігання дані мають бути надійно знищені або повністю анонімізовані.
- Періоди зберігання мають бути задокументовані та обґрунтовані.
- Пам'ятайте, що дані також можуть зберігатися в мобільних системах збору даних. Усі міркування зі зберігання даних, зазначені вище, застосовні і до мобільних систем збору даних.

Аналіз даних

- Існує протокол для обміну даними з консультантами, командами штаб-квартири, партнерами, зацікавленими сторонами, що включає, крім іншого, угоди про обмін даними, затвердження MEL країни, ролі та обов'язки тощо.
- Угоди про нерозголошення (NDA) підписуються всіма консультантами до отримання доступу до будь-яких наборів даних Mercy Corps.

Передача даних донору, партнеру або іншій третій стороні (за необхідності)

- Необроблені дані не ідентифікуються та перевіряються на відповідність принципам "Не нашкодь" перед відправкою.
- Конфіденційні дані не повинні передаватися третім особам, які не були згадані у процесі отримання поінформованої згоди.
- Конфіденційні дані не повинні передаватися третім особам, якщо не укладено угоду про спільне використання даних.
- Для обміну документами використовуйте лише авторизовані організаційні системи, такі як Google Drive або Microsoft Sharepoint, а не сторонні платформи обміну.

Поширені запитання

Щоб забезпечити дотримання вимог культурного різноманіття, ми просимо членів колективу вказувати свій етнічний статус в анкетах під час прийому на роботу – чи потрібно мені щось робити?

Так, дані про расове або етнічне походження вважаються конфіденційними персональними даними, тому вам необхідно дотримуватися рекомендацій щодо роботи з конфіденційними даними та застосовувати додаткові запобіжні заходи щодо цих даних.

Що трапиться, якщо я чи член моєї команди випадково, ненавмисно поділився конфіденційними даними? Яких заходів щодо виправлення ситуації можна вжити?

При виявленні випадкового обміну персональними даними, обмін даними має бути негайно припинено. Це може означати прохання випадкового одержувача видалити всі копії даних, видалення доступу випадкового одержувача до даних, переведення даних в автономний режим або інші необхідні заходи.

Випадкове або ненавмисне поширення персональних даних вважається порушенням даних, і ви повинні повідомити про це за адресою **it-security@mercycorps.org** негайно, відповідно до Плану реагування на інциденти. Необхідно якнайшвидше надати якомога більше інформації про характер даних, що передаються.

Що мені робити, якщо я бачу, що член команди навмисно ділиться конфіденційними даними з тим, хто не повинен мати до них доступу?

Умисна передача конфіденційних даних неуповноваженій особі є надзвичайно серйозною справою, оскільки може призвести до серйозних збитків як для суб'єкта даних, так і для агентства. Якщо ви бачите, що член команди навмисно ділиться конфіденційною інформацією таким чином, ви повинні негайно повідомити про це керівника програми, регіонального директора або свого директора.

Обмін конфіденційними даними з тими, хто не повинен мати до них доступ, також є порушенням даних, і про нього слід негайно повідомити на **it-security@mercycorps.org,** відповідно до Плану реагування на інциденти. Необхідно якнайшвидше надати якомога більше інформації про характер даних, що передаються.

Як програма вирішує, хто повинен/не повинен мати доступ до конфіденційних даних?

Доступ до конфіденційних даних повинен надаватися лише тим особам, яким він необхідний для виконання їх функцій. Конфіденційні дані, по можливості, завжди слід маскувати перед тим, як надати їх у спільний доступ. Звичайні приклади маскування включають анонімізацію або псевдонімізацію.

Що таке дисоційовані дані?

Дисоційовані дані - це дані, які були повністю та незворотно відокремлені від суб'єкта даних таким чином, що повторна асоціація даних із суб'єктом даних вже неможлива. Дисоційовані дані – це один із видів анонімізації даних.

Чи маю я ввімкнути попередження для електронного збору даних, якщо до нього матиме доступ неавторизована особа?

Якщо є можливість запускати сповіщення про несанкціонований доступ, їх завжди слід вмикати, проте не всі електронні платформи мають таку можливість. Перевірте налаштування вашої платформи і, якщо це можливо, увімкніть сповіщення.

Чи повинні члени команди використовувати особисті пристрої для збору або зберігання конфіденційної інформації? Якщо так, то які заходи захисту мають бути передбачені?

Персональні пристрої не повинні використовуватися для збору або зберігання особистої інформації, у тому числі інформації про учасників, *якщо тільки не встановлено відповідне програмне забезпечення для керування пристроями* та використання персональних пристроїв не зафіксовано у проекті PIA. Особисті пристрої ніколи не повинні використовуватися для збору даних учасників без спеціального дозволу керівника програми. Особисті пристрої не повинні використовуватися для збору або зберігання конфіденційної інформації.

Чи може мій донор перевірити, як я обробляю конфіденційні дані?

Так, багато донорів вимагають проведення внутрішніх, а також зовнішніх аудитів якості даних та оцінок якості даних. Одним із аспектів цих оцінок є оцінка системи MEL щодо потрясінь, вторгнень та безпеки, особливо якщо програма збирає конфіденційну інформацію.

Чи пов'язувати списки учасників з TolaData як доказ?

Списки учасників (наприклад, списки відвідуваності тренінгів тощо) можуть бути пов'язані як докази, оскільки ці докази повинні розміщуватися та зберігатися поза TolaData, таким чином, лише певні люди матимуть доступ до цих доказів, ґрунтуючись на дозволах цього зовнішнього сховища. Слід розглянути питання, чи вимагає будь-який вид доказів, пов'язаних з TolaData, вміст Персональної інформації. Вкрай малоймовірно, що буде потрібно додавати конфіденційну інформацію.

Як дізнатися, чи відповідають постачальники або платформи технологій збору або зберігання даних вимогам до конфіденційних даних?

Існуючі платформи збору та зберігання даних у MEL Tech Suite вже відповідають вимогам до конфіденційних даних, за умови, що вони відповідним чином налаштовані для використання гарантій та протоколів, зазначених у цьому документі. У разі використання платформи, що не входить до MEL Tech Suite, необхідно провести оцінку впливу на конфіденційність (PIA), щоб визначити, чи можна вважати її відповідною до конфіденційних даних. Щодо оцінки постачальника технологій та його готовності відповідати політиці відповідального використання даних та вимогам щодо конфіденційних даних, PIA знову є найкращим інструментом для визначення того, чи буде його практика відповідною до вимог.

Як визначити, чи є дані персональними чи конфіденційними?

Якщо ви обробляєте дані, які підпадають під одну зі спеціальних категорій конфіденційних даних, описаних у GDPR (див. розділ **"Спеціальні категорії конфіденційних даних"** вище), це завжди будуть конфіденційні дані. Якщо існує специфічна причина, через яку дані потрапляють у категорію даних "підвищеної конфіденційності" (див. Малюнок 1 вище), їх також слід класифікувати як конфіденційні дані.

Супутні документи:

Згода

Інструмент MEL: Шаблон інформованої згоди (для учасників інтерв'ю)

Посібник з інформованої згоди для спільного використання даних CARM

COVID-19 Дистанційний посібник MERL

Шифрування

Використання Ona.io у Mercy Corps: Шифрування форм та конфіденційних даних

Біометрія

Біометрія @ Mercy Corps: Внутрішня первинна обробка

Загальні рекомендації

- Посібник з відповідальності за роботу з даними - Інструкції для практиків у галузі готівки та ваучерів - https://www.calpnetwork.org/wp-content/uploads/2021/03/Data-Responsibility-Toolkit_A-guide-for-Cash-and-Voucher-Practitioners.pdf
- Початковий комплект даних ELAN для гуманітарного персоналу на місцях: https://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf
- Посібник МКЧХ із захисту даних у гуманітарній діяльності: https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

Деідентифікуюча інформація

Інструкції Міністерства сільського господарства США щодо розгляду персонально ідентифікованої інформації (PII) при оцінці проектів

Експертна група по боротьбі з бідністю 'Деідентифікація для публікації даних'

Генерація унікальних кодів для учасників програми чи інших суб'єктів даних

Проект рекомендацій від T4D

Оціночні показники

Оцінка впливу на конфіденційність (PIA)- шаблон

Оцінка впливу на конфіденційність (PIA)- Посібник

Оцінка конфіденційної інформації (SIA)