Использование «закрытых» данных

Руководство по обработке закрытых данных

Содержание

Обоснование

В рамках большинства программ и другой деятельности Mercy Corps собирает ту или иную персональную информацию о людях, которым организация помогает и с которыми работает, и может также собирать информацию о людях, которую можно рассматривать как закрытую. Сбор закрытой информации крайне важен для выполняемой нами работы и оказания помощи участникам программ и сообществам. Таким образом, при сборе и использовании закрытой информации крайне важно принимать надлежащие меры по защите таких данных. Незащищенность закрытых данных может привести к серьезным негативным последствиям для субъекта данных, включая, среди прочего, дискриминацию и угрозы безопасности.

Содержание

Настоящее руководство применяется к любой обработке закрытых данных в пределах организации. Руководство действует в отношении данных, собранных в целях реализации программ и деятельности, а также в отношении других ситуаций с вовлечением закрытых данных. Настоящий документ подробно описывает необходимые действия в рамках обработки закрытой информации.

Что такое «закрытые данные» и чем они отличаются от других видов персональных данных?

Как правило, закрытые данные — это такие данные, как культурные характеристики, сексуальная ориентация, данные о состоянии здоровья, биометрические и генетические данные. Это данные, ненадлежащее раскрытие, доступ и передача которых могут привести к следующему:

- вред (например санкции, дискриминация и угрозы безопасности) человеку, включая источник информации или других лиц и группы, которые могут быть распознаны;
- негативное влияние на способность организации осуществлять деятельность или восприятие организации общественностью.

Пример 1:

В сообществе реализуется программа, а в ходе проекта несколько участников признаются, что у них ВИЧ. Эта информация случайно становится известной старшим членам сообщества, что приводит потенциально к нанесению серьезного ущерба или даже к угрозе физической расправы над участниками программы.

Пример 2:

В офисе планируется торжество, а члены команды должны сообщить о своих требованиях к блюдам. Несколько членов сообщают, что им нужны кошерные либо халяльные блюда. Документ, в котором указано, кто из членов команды имеет особые требования к блюдам, попадает в распоряжение всей команды. Некоторые члены команды не указали свою религию, поскольку боялись дискриминации.

Обращение с закрытой информацией требует особой осторожности, поскольку, по всей вероятности, сбор и использование такой информации нарушают основные права или свободы человека или приводят к нанесению серьезного ущерба, включая дискриминацию или физическую опасность, при неправильном обращении с ней.

В Общем регламенте по защите данных (GDPR) определен ряд видов данных, которые отнесены к особой категории закрытых данных, и описываются особые условия обработки таких видов данных. Тем не менее, важно обратить внимание на то, что в некоторых ситуациях данные, которые не относятся к стандартной категории закрытых данных, могут быть закрытыми в силу тех или иных обстоятельств. В рамках настоящего руководства такие виды данных называют «контекстуально закрытые данные».

Настоящее руководство дополняет Политику по ответственному отношению к данным Mercy Corps и Политику управления программами (которая включает также Политику MEL организации) и применяется к сбору закрытых данных в любых обстоятельствах, включая головной офис, программы и MEL.

Определение ключевых терминов

- **Оперативные данные Mercy Corps** – любая единица информации, состоящая из букв, чисел, символов, изображений, видео и записей речи, геопространственных координат или обозначения местоположения, карты либо их сочетания, обрабатываемая Mercy Corps. Сюда могут относиться данные членов команды, поставщиков, спонсоров или партнеров Mercy Corps. Данные существуют как в цифровом, так и в физическом виде.

- **Закрытый данные.** Эта информация часто используется как основа целенаправленной работы с определенной группой или человеком. Типичные примеры — раса, религия, политические взгляды, сексуальная ориентация, информация о состоянии здоровья или биометрических данных.

  В рамках настоящего руководства закрытые данные включают особую категорию закрытых данных (см. GDPR) и контекстуально закрытые данные.

- **Особая категория закрытых данных.** В GDPR указаны особые требования к обработке всех закрытых данных из особой категории, которые должны соблюдаться. В соответствии с GDPR особая категория закрытых данных — это:

  - персональные данные, раскрывающие расу или этническую принадлежность;
  - персональные данные, раскрывающие политические взгляды;
  - персональные данные, раскрывающие религиозные или философские взгляды;
  - персональные данные, раскрывающие участие в профсоюзах;
  - генетические данные;
  - биометрические данные (если они используются для идентификации);
  - данные о состоянии здоровья;
  - данные о сексуальной жизни и
  - данные о сексуальной ориентации.

- **Контекстуально закрытые данные —** данные, которые не являются закрытыми в соответствии с GDPR, но которые в силу обстоятельств, в которых происходит их обработка, являются закрытыми по своему характеру и при их раскрытии могут нанести вред субъекту данных.

- **Нарушение, связанное с персональными данными**. В широком смысле нарушение, связанное с персональными данными, – это нарушение безопасности, затрагивающее конфиденциальность, целостность или доступность персональных данных. Словом,

нарушение, связанное с персональными данными, имеет место в случае утери, уничтожения, повреждения или раскрытия данных, если какое-либо лицо получает доступ к данным или передает данные без надлежащего разрешения или если данные становятся недоступными, например, при их шифровании программами, требующими выкуп, или непреднамеренной потере или уничтожении.

- **Данные о программе** – любая единица информации, состоящая из букв, чисел, символов, изображений, видео и записей речи либо их сочетания, которая имеет отношение к участникам, реализации и результатам программы. Данные существуют как в цифровом, так и в физическом виде.

- **Политика по ответственному отношению к данным Mercy Corps** – политика организации, устанавливающая принципы прозрачности, безопасности и ответственного использования персональных данных в рамках организации и внедряющая такие принципы в повседневную работу.

- **Информированное согласие** – процесс получения от участников добровольного разрешения на сбор любых данных на основании четкой оценки, понимания фактов и последствий участия. Согласие может быть письменным, устным или в форме аффирмативного действия. Согласие необходимо получить в момент сбора персональных данных либо сразу же после этого.

- **Явно выраженное согласие**. Явно выраженное согласие подразумевает очень четкое и однозначно выраженное согласие. Необходимо зафиксировать дату и способ получения согласия и указать, что конкретно было сообщено субъектам данных при получении согласия. В явно выраженном согласии должен быть указан характер данных из специальной категории, а согласие должно быть получено отдельно от других согласий.

- **Обезличивание данных** — любые методы или действия по обработке данных, направленные на предотвращение прямого и/или косвенного раскрытия личности участника или иного лица. Примеры: анонимизация (т. е. удаление определенного объема персональных данных или применение ряда значений в отношении определенных наборов персональных данных) и псевдонимизация (т. е. обработка персональных данных, после которой больше невозможно установить принадлежность персональных данных к конкретному субъекту или группе субъектов без использования дополнительной информации, например уникального идентификационного номера или набора символов).

- **Персональные данные, позволяющие идентифицировать личность (PII)**, – любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъекту данных); идентифицируемое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, на основе идентификационного номера или по одному или нескольким показателям, характерным для физической, физиологической, психической, экономической, культурной или социальной идентичности данного физического лица. Это понятие тесно связано с **данными, позволяющими идентифицировать демографические признаки (DII)**, т. е. данными, которые могут использоваться для идентификации сообщества или отдельной группы людей по географическим, этническим, религиозным, экономическим или политическим признакам.

- **Безопасное хранение.** Только соответствующие сотрудники Mercy Corps могут получить доступ к данным, при этом принимаются меры для предотвращения кражи и неправильного использования данных. Безопасное хранение. Хранение файла является безопасным в следующих случаях:
  - файл находится на платформе, которая отвечает строгим стандартам по безопасности, защите данных и конфиденциальности;
  - доступ имеют исключительно уполномоченные лица;
  - доступ постоянно анализируется, при необходимости вносятся изменения.

- Дополнительные требования установлены для программ Mercy Corps в недавно принятой Политике MEL. В частности, в соответствии со Стандартом 9 все программы должны обеспечить безопасное обращение в соответствии с Политикой по ответственному отношению к данным и требованиями спонсора.

- **Необходимые члены команды Mercy Corps** – члены команды, которым необходим доступ к указанной информации для выполнения должностных обязанностей, например, для помощи участникам программы и достижения целей программы.

- **Субъект данных** — любое физическое лицо, данные которого получают напрямую, косвенно или через третье лицо и которое может быть идентифицировано прямо или косвенно, в частности, путем ссылки на персональные данные.

- **Защита данных** — защита и предотвращение несанкционированного доступа, использования или распространения персональных данных, позволяющих идентифицировать личность (PII), данных, позволяющих идентифицировать демографические признаки (DII), или другой закрытой информации о физическом лице или группе в рамках данных об управлении программой или проектом либо после завершения программы или проекта. Политикой Mercy Corps по ответственному отношению к данным определены требования по защите данных; кроме того, в отношении организации действуют другие законодательные/регуляторные требования, например Общий регламент ЕС по защите данных (GDPR).

Другие термины и определения, касающиеся ответственного отношения к данным, см. в документе «Термины и определения, имеющие отношение к ответственному отношению к данным».

Планирование

- Проанализируйте, какие виды данных будут собираться, и зафиксируйте информацию на этапе планирования проекта, в Оценке влияния на конфиденциальность (PIA).

- Если план предусматривает сбор и/или документирование и/или хранение любых закрытых данных, особое внимание следует уделить способу и основаниям для использования данных. Проанализируйте, необходим ли сбор данных для достижения заданных целей программы или проекта или же достаточно данных другого вида. Закрытая информация собирается только в случае крайней необходимости. Обратите внимание, что надлежащий сбор закрытых данных требует значительных затрат. Исключая необходимость сбора ненужных данных, вы экономите время и ресурсы для другой важной деятельности. Если необходимы PII, не прибегайте к

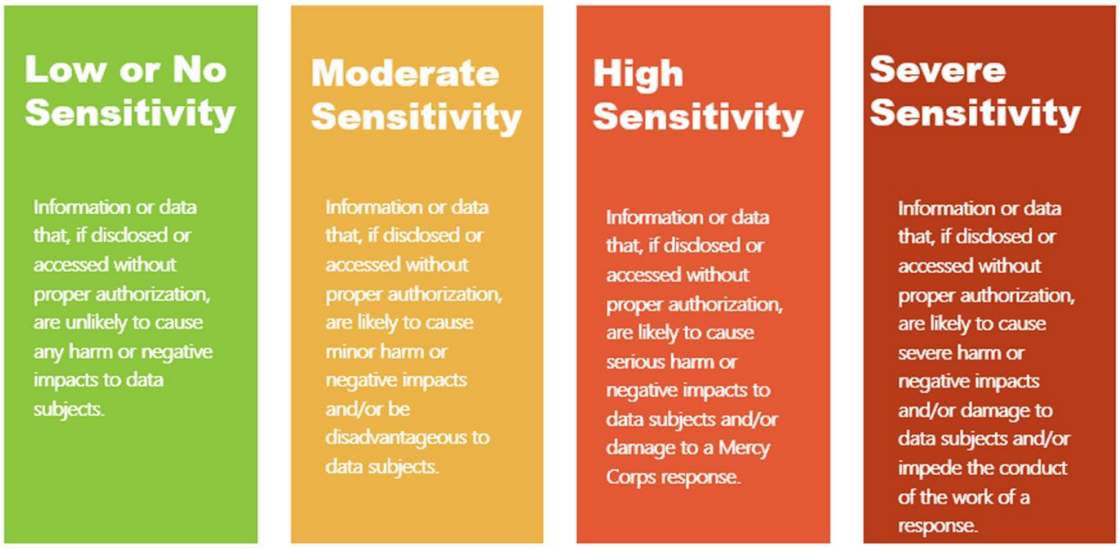
сокращению. Если ресурсов, привлеченных для сбора и управления закрытыми данными, недостаточно для обеспечения надлежащего процесса, учтите все риски для сообществ, с которыми вы работаете.

- Подумайте, какие технологии будут использоваться для сбора и хранения. Используемые технологии должны обеспечивать надлежащую защиту при сборе закрытой информации.
- В целом, чем чувствительнее данные, тем больше средств защиты они требуют. Как правило, закрытые данные могут быть «очень» или «крайне» закрытыми (см. рис. 1). Кроме того, чем больше массивов данных собрано, тем выше риск и тем больше средств защиты должно использоваться. Некоторые примеры средств защиты:
    - шифрование;
    - псевдонимизация;
    - устранение связи;
    - хранение файлов на бумажном носителе в закрытых шкафах с ограничением доступа;
    - хранение файлов на серверах Mercy Corps с несколькими степенями защиты;
    - ограничение доступа к устройствам Mercy Corps и предоставление доступа только тем лицам, которым доступ необходим для выполнения должностных обязанностей;
    - блокировка устройств, например ноутбуков, когда они не используются;
    - для геопространственных данных — рандомизация или агрегация GPS-точек.

- Четко определите, какие правовые основания для обработки закрытых данных вы будете использовать, и составьте план, исходя из этого.
- Установление требований в соглашениях о грантах должно соответствовать принципу «Не навреди» (например, в рамках программы не предполагается собирать информацию, которая может поставить под угрозу безопасность участников); должны четко определяться обязательства и договоренности для платформ обмена информацией, процессов со спонсорами, партнерами и другими заинтересованными лицами, включения требований по обезличиванию данных и анонимизации.
- Протокол безопасности данных на уровне программы является частью Плана по технологии MEL (Стандарт 6) и определяет принципы действий членов команды в отношении данных, включая уровни доступа и протоколы для членов команды из MC и сторонних членов.
- Если закрытые данные собираются для целей деятельности Mercy Corps, необходимо спланировать и определить принципы в отношении данных, включая уровни доступа и протоколы.
- Подумайте и будьте готовы обосновать продолжительность хранения данных (период хранения), которая будет зависеть от причин для сбора информации, юридических требований, требований спонсора и политики по хранению для программ MC.

- Следует определить процесс уничтожения данных по истечении периода хранения.

Рис. 1.



Планирование сбора данных

- Оценка влияния на конфиденциальность выполняется для выявления и управления рисками нарушения конфиденциальности данных, связанными с любой новой деятельностью, например программами, технологиями или мерами в рамках политики. При необходимости сбора закрытых данных анализ проводится компетентным лицом: сотрудником отдела защиты данных и конфиденциальности, вашим главным специалистом по защите данных или по Политике MEL (Минимальный стандарт №9 «Защита данных и конфиденциальность»):
    - Отчитывающееся лицо: руководитель по стране, руководитель программ, менеджер проекта или руководитель проекта
    - Рекомендуемое ответственное лицо: MEL программы/ главный специалист по управлению данными

- Выполните оценку закрытой информации (SIA), связанной с оценкой влияния на конфиденциальность. Здесь необходимо указать все дополнительные средства защиты, используемые для закрытых данных.

- Если законом предусмотрено получение согласия, получение информированного согласия предполагает сообщение следующей информации субъектам данных понятным языком:

    - какие данные собираются и для чего это нужно;

    - кому данные будут предоставляться, включая внешних партнеров и спонсоров;

    - будут ли данные передаваться по всему миру;
    - продолжительность хранения данных;
- следует зафиксировать, когда и каким образом было получено согласие и что было сказано субъекту данных. На этапе планирования следует включить образец информации, которая будет предоставляться субъекту данных при получении согласия.

Сбор данных

- Для каждого случая сбора данных используется протокол сбора данных, который включает:
    - дополнительные средства защиты для закрытых данных;
    - письменные инструкции по сбору, очистке данных, пересмотру и обезличиванию данных (если необходимо);
    - инструкции на случай возможных нарушений безопасности данных для всех собранных количественных и качественных данных (например, утерянные или украденные устройства, взломанные имена пользователей и пр.);
    - инструкции по использованию и защите бумажных носителей информации в процессе сбора;
    - выборочные проверки и мониторинг степени соблюдения правил лицами, собирающими данные, средств и протоколов защиты;
- все вышеуказанное должно быть привязано к SIA.

Хранение данных

- Доступ к файлам, содержащим закрытую информацию, должен предоставляться только сотрудникам, которым доступ к такой информации необходим для достижения поставленных целей; обезличивание данных в закрытой информации выполняется до привязки к TolaData или предоставления третьей стороне. Политика MEL, Стандарт 8, содержит дополнительное руководство по подаче и хранению данных MEL.
- Данные хранятся в месте, которое отвечает соответствующим положениям Mercy Corps (например, Положение по ответственному отношению к данным, руководство «Допустимое использование»).
- Закрытые данные хранятся не дольше необходимого срока. По истечении периода хранения данные должны быть уничтожены или полностью анонимизированы.
- Продолжительность хранения должна быть задокументирована и обоснована.
- Обратите внимание, что данные могут храниться также в мобильных системах сбора данных. Все указанные требования применяются в равной степени к мобильным системам сбора данных.

Анализ данных

- Разработан протокол передачи данных консультантам, сотрудникам головного офиса, партнерам, заинтересованным лицам, включая, среди прочего, утверждение MEL по стране, роли, обязанности и пр.

- Соглашение о неразглашении информации (NDA) подписывается всеми консультантами до предоставления доступа к любым базам данных, принадлежащим Mercy Corps.

Передача данных спонсору, партнеру или третьей стороне (если применимо)

- Перед передачей необработанные данные обезличиваются и анализируются на предмет соблюдения принципа «Не навреди».

- Закрытые данные не передаются какой-либо третьей стороне, которая не указана в информированном согласии.

- Закрытые данные передаются какой-либо третьей стороне только при наличии Соглашения об обмене данными.

- Для передачи документов следует использовать авторизованные организационные системы, такие как Google Drive или Microsoft Sharepoint, а не сторонние платформы.

Часто задаваемые вопросы

Чтобы обеспечить соблюдение требований по этническому и социокультурному многообразию, мы просим членов команды указать этническую принадлежность в анкете. Мне нужно что-то с этим делать?

Да, данные о расе или этнической принадлежности являются закрытыми персональными данными, поэтому следует придерживаться руководства по закрытым данным и использовать дополнительные средства защиты в отношении таких данных.

Что случится, если я или член команды случайно, непреднамеренно раскроем закрытые данные? Каким образом можно исправить ситуацию?

Если становится известно о случайном разглашении персональных данных, разглашение необходимо прекратить немедленно: например, попросить случайного получателя данных удалить все копии данных, закрыть случайному получателю доступ к данным, перевести данные в режим оффлайн или принять другие меры.

Случайное или непреднамеренное раскрытие данных считается нарушением в отношении данных, и о нем необходимо немедленно сообщить по адресу **it-security@mercycorps.org** в соответствии с

Планом реагирования на происшествия. Следует предоставить как можно больше информации о характере раскрытой информации в максимально короткие сроки.

Что делать, если я вижу, как член команды преднамеренно передает закрытую информацию кому-то, кто не должен получать такую информацию?

Преднамеренная передача закрытой информации не уполномоченному лицу является крайне серьезным нарушением, поскольку может повлечь негативные последствия для субъекта данных и организации. Если вы видите, как член команды передает закрытую информацию подобным образом, следует немедленно сообщить об этом руководителю проекта, региональному директору или вашему непосредственному руководителю.

Предоставление закрытой информации кому-либо, кто не должен иметь доступ к данным, считается нарушением в отношении данных, и об этом необходимо немедленно сообщить по адресу **it-security@mercycorps.org** в соответствии с Планом реагирования на происшествия. Следует предоставить как можно больше информации о характере раскрытой информации в максимально короткие сроки.

Каким образом принимается решение о том, кто имеет, а кто не имеет доступ к закрытым данным по программе?

Доступ к закрытым данным должен предоставляться исключительно тем лицам, которым такая информация необходима для выполнения должностных обязанностей. Если возможно, перед раскрытием закрытые данные должны маскироваться (анонимизация и псевдонимизация).

Что такое «разъединенные данные»?

Разъединенные данные — это данные, которые полностью и безвозвратно отделены от субъекта данных, и больше не представляется возможным связать данные с субъектом данных. Разъединенные данные — это разновидность анонимизации.

Следует ли активировать сигнал тревоги по электронным массивам данных в случае доступа неуполномоченного лица?

Если есть возможность активировать оповещение в случае несанкционированного доступа, его необходимо включать, однако, не все электронные платформы предлагают такую функцию. Проверьте настройки системы на вашей платформе и, если возможно, активируйте тревогу.

Должны ли члены команды пользоваться персональными устройствами для сбора и хранения закрытой информации? Если да, то какие средства защиты должны использоваться?

Не следует использовать персональные устройства для сбора и хранения персональной информации, включая информацию об участнике; *исключение составляют ситуации, когда установлено необходимое программное обеспечение для управления устройством,* а использование персональных устройств указано в PIA по проекту. Персональные устройства ни в коем случае не

должны использоваться для сбора данных об участнике без разрешения руководителя программы. Персональные устройства не должны использоваться для сбора и хранения закрытой информации.

Может ли спонсор проверить, как я обращаюсь с закрытой информацией?

Да, многие спонсоры требуют проводить внутренние и внешние аудиты качества данных и оценки качества данных. Одной из целей таких оценок является анализ системы MEL на предмет нарушений, взломов и обеспечения безопасности, особенно если в рамках программы собирается закрытая информация.

Следует ли привязывать списки участников к TolaData в качестве доказательства?

Списки участников (например списки участников тренингов и т. п.) могут использоваться в качестве доказательства, но должны находиться и храниться за пределами TolaData, чтобы только определенные лица имели доступ к такому доказательству, с учетом разрешений в такой внешней системе хранения. Следует проанализировать, необходимо ли включать персональную информацию в какой-либо вид доказательства, привязанного к TolaData. Очень маловероятно, что потребуется включить персональную информацию.

Как узнать, соблюдают ли поставщики технологий или платформ для сбора или хранения требования по закрытой информации?

Существующие платформы для сбора и хранения данных в пакете MEL Tech Suite отвечают требованиям по закрытой информации, при условии правильных настроек средств защиты и протоколов, упомянутых в настоящем документе. При использовании платформы, не включенной в MEL Tech Suite, следует выполнить оценку влияния на конфиденциальность (PIA), чтобы установить, соответствует ли платформа требованиям по закрытым данным. Что касается поставщиков технологий и их желания соблюдать Политику по ответственному отношению к данным и требования по закрытой информации, то и здесь PIA является лучшим инструментом для определения их соответствия.

Каким образом определить, что данные являются персональными или закрытыми?

Если вы обрабатываете данные, которые относятся к особой категории закрытых данных, указанной в GDPR (см. выше **«Особая категория закрытых данных»**), это всегда будут закрытые данные. Если, исходя из контекста, есть основания полагать, что данные будут отнесены к «крайне закрытым» данным (см. выше рис. 1), их также следует отнести к закрытым данным.

Документы по теме:

Согласие

Инструмент MEL: образец информированного согласия (для участников интервью)

Руководство по информированному согласию при обмене данными CARM

Руководство по удаленному MERL во время эпидемии COVID-19

Шифрование

Использование Ona.io в Mercy Corps: формы шифрования и закрытые данные

Биометрические данные

Биометрические данные в Mercy Corps: внутреннее руководство

Общие руководства

- Пакет данных для ответственного отношения к данным: руководство для участников программы Cash and Voucher https://www.calpnetwork.org/wp-content/uploads/2021/03/Data-Responsibility-Toolkit_A-guide-for-Cash-and-Voucher-Practitioners.pdf
- Базовый комплект ELAN Data Starter Kit для сотрудников гуманитарных программ на месте: https://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf
- Руководство Международного комитета Красного Креста (ICRC) по защите данных в гуманитарных проектах: https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

Обезличивание информации

Руководство USDA по анализу персональных данных, позволяющих идентифицировать личность (PII), при оценке проекта

Руководство программы по борьбе с бедностью «Обезличивание информации для публикации данных»

Генерирование уникальных кодов для участников программ или других субъектов данных

Проект руководства T4D

Оценки

Образец оценки влияния на конфиденциальность (PIA)

Руководство по оценке влияния на конфиденциальность (PIA)

Оценка закрытой информации (SIA)