Data Protection is ***People*** *Protection*

РУКОВОДСТВА ПО ЗАЩИТЕ ДАННЫХ И КОНФИДЕНЦИАЛЬНОСТИ

MERCY CORPS

Следующий контент предназначен для того, чтобы помочь сотрудникам Mercy Corps лучше понимать и внедрять методы ответственного обращения с данными. Он включает несколько существующих политик и руководств Mercy Corps, а также некоторые простые учебные пособия и ссылки на другие ресурсы. Вся информация может быть использована как одно всеобъемлющее руководство, или каждый раздел может использоваться как отдельное руководство по определенной теме.

Хотя это руководство в первую очередь предназначено для сотрудников Mercy Corps и дополняет **Инструментарий по ответственному обращению с данными**, мы выпускаем его в качестве открытого ресурса, чтобы оно могло быть полезно партнерам и другим организациям, а также третьим сторонам, которым могут потребоваться примеры политик, шаблонов и инструкций по внедрению методов ответственного обращения с данными. Вы можете скачать все содержимое нашего руководства на нашей странице Github по адресу **https://github.com/mercycorps/DPP-guides**.

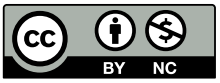
Оглавление

Цитаты и благодарности

Содержимое, представленное в этом руководстве, является частью передовой практики управления данными и более широкого жизненного цикла данных или общих действий по управлению отдельными данными в рамках программной деятельности или реагирования. Следующие ресурсы можно использовать как эффективные отправные точки для более полного понимания ответственного управления вашими данными. Мы использовали или цитировали части всех этих ресурсов в Руководстве и ссылались на определенные главы или разделы, наиболее релевантные к определенной теме.

- Инструментарий по ответственному обращению с данными от Партнерства по обучению обращения с наличными деньгами (Cash Learning Partnership) разработан непосредственно для специалистов, работающих с наличными и ваучерами и является золотым стандартом в руководстве по ответственным данным. Инструментарий доступен на английском, арабском, французском и испанском языках.
- Стартовый комплект данных для полевого гуманитарного персонала Сообщества для активного обучения электронным денежным переводам (Electronic Cash Transfer Learning Action Network) содержит материалы для разъяснения различных аспектов надлежащего управления данными и методов защиты.
- Руководство по защите данных в гуманитарной деятельности Международного комитета Красного Креста представляет собой подробное руководство практически по всем аспектам гуманитарных данных.
- Методичка по использованию данных (Data Playbook) Международной Федерации обществ Красного Креста и Красного Полумесяца (IFRC) — это отличный источник упражнений, планов занятий, контрольных списков и других материалов, которые помогут вам организовать дискуссии и мероприятия с вашей командой на тему ответственного обращения с данными.
- Учебное онлайн-руководство по проведению оценки риска раскрытия информации Центра гуманитарных данных — это очень специфический технический ресурс, но он незаменим для реального снижения риска при использовании данных для установления личности.
- Справочник современного специалиста в области развития от Engine Room — хороший обзор данных в контексте работы в области международного развития.

Лицензия



Понимание закрытых («чувствительных» данных)

Понимание различных классификаций данных может показаться затруднительным, но они являются важной частью работы с гуманитарными данными. Например, в чем разница между личными данными и закрытыми («чувствительными») данными? Определенные типы данных могут требовать особого обращения в соответствии с региональными или национальными законами или политиками организации, так как могут представлять различные виды риска как для участников программы, так и для организаций. Закрытые («чувствительные») данные — это подкатегория персональных данных. В этом разделе содержится подробное руководство по их обработке и разъяснению.

☆ Важность

Большинство программ Mercy Corps и других процессов собирают определенную личную информацию о людях. Во многих случаях программы также собирают информацию о культурном профиле человека, его/ее сексуальной ориентации, здоровье, или данные биометрического/генетического характера. Эти виды информации считаются закрытыми («чувствительными») данными, и их неправомерное раскрытие, доступ или совместное использование могут привести к:

- нанесению вреда человеку, такого как санкции, дискриминация и угрозы безопасности;
- негативному влиянию на деятельность Mercy Corps, снижению доверия или общественного восприятия.

Крайне важно предпринять необходимые шаги для защиты этих данных.

Руководство

Этот раздел содержит два документа:

- «Руководство по обработке закрытых («чувствительных») данных» знакомит вас с закрытыми данными, ключевыми терминами и тем, что следует учитывать при планировании их сбора, хранения, анализа и обмена.
  - Сотрудники Mercy Corps могут получить доступ к Руководству во внутренней цифровой библиотеке Mercy Corps.
  - Любой желающий может скачать руководство на английском, арабском, испанском, французском и русском языках.
- «Шаблон оценки закрытой («чувствительной») информации (SIA)» можно использовать с оценкой воздействия на конфиденциальность для документирования всех дополнительных мер безопасности, используемых для закрытых данных. В этом документе также изложены различные правовые основы, которые могут использоваться для оправдания сбора и использования закрытых данных.
  - Сотрудники Mercy Corps могут получить доступ к шаблону SIA во внутренней цифровой библиотеке Mercy Corps.
  - Любой может скачать шаблон в виде документа Microsoft Word на английском, арабском, испанском, французском и русском языках.

Дальнейшая помощь

Планирование сбора или использования закрытых («чувствительных») данных должно быть частью более широкой стратегии жизненного цикла данных программы или процесса. Есть несколько ресурсов, которые могут быть вам полезны.

- Методичка по использованию данных (Data Playbook) Международной Федерации обществ Красного Креста и Красного Полумесяца (IFRC) — это отличный источник упражнений, планов занятий, контрольных списков и других материалов, которые помогут вам организовать дискуссии и мероприятия с вашей командой на тему ответственного обращения с данными. В частности, рекомендуем Модуль 4 — Ответственное отношение к данным как хорошую отправную точку.
- *Руководство по защите данных в гуманитарной деятельности* Международного комитета Красного Креста представляет собой подробное руководство практически по всем аспектам гуманитарных данных. В главе 3 конкретно рассматриваются правовые основы обработки персональных данных.
- Инструментарий по ответственному обращению с данными от Партнерства по обучению обращения с наличными деньгами (Cash Learning Partnership) разработан непосредственно для специалистов, работающих с наличными и ваучерами и является золотым стандартом в руководстве по ответственным данным. В частности, *в разделах Список подсказок #2, "Дизайн и планирование"* обсуждаются законные основания для закрытых («чувствительных») данных. Инструментарий доступен на английском, арабском, французском и испанском языках.

Оценка влияния на конфиденциальность

Это руководство поможет вам разобраться в оценке влияния на конфиденциальность (PIA). Оно содержит правила PIA и шаблон, используемые в Mercy Corps. Шаблон PIA содержит ряд вопросов, создающих основу для выявления потенциальных рисков для конфиденциальности, связанных со сбором данных, которые являются частью внедрения новой программы или технологии, а также управлением этими данными. PIA также имеет значение, когда контекст программы значительно меняется, и необходимо учитывать новые риски или сценарии.

PIA требуется для каждой новой программы, проекта или технологии, которые связаны со сбором или использованием личных или «чувствительных» данных.

☆ Важность

PIA позволяет вам проанализировать, как конкретный проект или новая технология повлияют на конфиденциальность вовлеченных лиц. PIA также помогает документировать стратегии смягчения последствий, которые защищают конфиденциальность участников и укрепляют доверие общества к нашей работе. PIA гарантирует, что потенциальные проблемы будут выявлены на ранней стадии, когда их решение будет более простым, менее затратным и не подвергнет риску участников программы или персонал.

Принципы

Принципы, лежащие в основе PIA, аналогичны принципам любого безопасного использования персональных данных. Ниже приведены некоторые ключевые принципы, адаптированные из Cash Learning Partnership (CaLP):

- Определите риски конфиденциальности для отдельных лиц.
- Определите обязательства вашей организации по соблюдению конфиденциальности и защите данных.
- Демонстрируйте подотчетность и соблюдение политик, защищающих участников программы, партнеров и персонал.
- Убедитесь, что в своей гуманитарной деятельности организация продвигает право на неприкосновенность частной жизни и распоряжается данными, руководствуясь этическими нормами.

Руководство

Сотрудники Mercy Corps могут найти Руководство по PIA в цифровой библиотеке. Документ содержит ответы на часто задаваемые вопросы, связанные с PIA, и ссылки на внутренний архив Mercy Corps с завершенными PIA для сравнения. Руководство Mercy Corps по PIA доступно для всех на английском, арабском, испанском, французском и русском языках.

Помните, что:

- PIA — это *процесс*, используемый для выявления и сведения к минимуму угроз, связанных с конфиденциальностью. Заполнение формы PIA — это не конечный шаг процесса! Повторно просмотрите PIA после запуска проекта, чтобы убедиться в отсутствии новых изменений, создающих новые угрозы. Если эти угрозы есть, зафиксируйте изменения и новые стратегии смягчения последствий, необходимые для минимизации любой новой угрозы.

- Проведение PIA предполагает работу с людьми из Mercy Corps, а иногда и с партнерскими и другими организациями для выявления и снижения угроз конфиденциальности. Например, если вы используете новую технологию, вам может потребоваться узнать о политике конфиденциальности вашего партнера и о том, какие технологические меры безопасности они используют для обеспечения защиты данных. Вам также может потребоваться узнать о соответствующих правилах конфиденциальности в вашей стране. Три веб-сайта, которые вы можете использовать для мониторинга данных национального уровня и законов о конфиденциальности:
  - Всемирные законы о защите данных;
  - База данных Конференции ООН по торговле и развитию о Защите данных и законах о конфиденциальности во всем мире; и
  - Единая база данных Trust Data Guidance по глобальным законам о конфиденциальности.
- Может быть полезно сравнить PIA похожих программ. Вы можете провести это исследование самостоятельно или обратиться за помощью к отделу по защите данных и конфиденциальности.

Шаблоны

Сотрудники Mercy Corps могут найти полную форму шаблона PIA в цифровой библиотеке. Полный шаблон PIA доступен для всех на английском, арабском, испанском, французском и русском языках.

Каждый полный шаблон PIA включает пять вариантов использования, которые объясняются ниже. Щелкнув по приведенным ниже ссылкам, вы попадете на экран, где любой желающий может скачать англоязычные версии отдельных вариантов использования в формате **.odt** (совместимые с Microsoft Word и приложениями с открытым исходным кодом, такими как OpenOffice и LibreOffice), выбрав опцию **Просмотр в необработанном виде** или **Скачать**.

- новая Политика
- новый Процесс или Процедура
- новая Программная или технологическая система
  - Это в первую очередь предназначено для внедрения новых систем на уровне всего мира, страны или коллектива.
  - Если вы выбираете или используете новую систему как часть более крупного проекта или программы, вместо этого используйте опцию проекта или программы.
- новый Поставщик или Партнер
  - Это в первую очередь предназначено для проверки действий поставщика, партнера или третьей стороны в рамках уникального или одноразового действия.
  - Если вы выбираете или используете нового поставщика, партнера или третью сторону в рамках более крупного проекта или программы, вместо этого используйте опцию Проект или Программа.
- новый Проект или Программа
  - Это может относиться к любому этапу или аспекту проекта или программы.
  - *Это наиболее полный вариант PIA*, который также включает язык для выбора нового программного обеспечения или технических систем и/или нового поставщика или партнера.

Дальнейшая помощь

- Стартовый комплект данных от Electronic Cash Transfer Learning Action Network содержит список подсказок для PIA **(см. список подсказок №1)**.
- Управление Комиссара по защите информации в Великобритании предоставляет подробный свод правил для проведения оценок влияния на конфиденциальность.
- *Руководство по защите данных в гуманитарной деятельности* Международного комитета Красного Креста представляет собой подробное руководство практически по всем аспектам гуманитарных данных. В главе 5 конкретно рассматриваются оценки влияния на конфиденциальность.

Рекомендации по совместному использования файлов

В этом руководстве описаны рекомендации по совместному использования файлов для членов команды Mercy Corps, использующих приложения G Suite, в частности Google My Drive. Чтобы упростить это руководство, мы будем обсуждать совместное использование одного конкретного *файла*, например, электронной таблицы. Однако при совместном использовании *папки* My Drive, доступны те же опции.

Примечание. Mercy Corps переходит на Microsoft 365 для совместного использования файлов. После того, как будут определены наилучшие практики для этой платформы, будет создан аналогичный документ или ресурс.

☆ Важность

Есть несколько причин, по которым лучше поделиться файлом, разместив его на Google Диске (Google Drive) и отправив ссылку, а не в виде вложения в электронном письме.

- Безопасность: вы можете легко выбирать, кому разрешены доступ или редактирование вашего файла. Вы также можете сделать ссылку, прикрепленной к временным рамкам, разрешив доступ к файлу только в течение определенного периода времени.
- Контроль версий: при совместном использовании файла, размещенного в Интернете, к нему могут получить одновременный доступ многие люди, и все изменения и комментарии останутся в одном файле. Отправка файла в виде вложения часто приводит к созданию нескольких версий одного и того же документа с разными именами файлов, правками, комментариями и т. д. Владелец документа потратит много времени, пытаясь скомпилировать все это в один файл! Использование ссылки также гарантирует, что получатели всегда будут иметь доступ к самой последней версии документа.
- Размеры файлов. Некоторые IT-отделы налагают ограничения на размер разрешенных вложений. Отправка ссылки позволяет обмениваться файлами любого размера.
- Простое редактирование: файлы, опубликованные как документы Google на Диске (Drive), Microsoft Word в OneDrive или в аналогичных форматах, позволяют получателю открывать документ и взаимодействовать с ним с помощью веб-браузера. Ему не обязательно иметь самую последнюю версию программного обеспечения определенного типа.

Принципы

Всякий раз, когда вы делитесь документами, вы должны учитывать следующее:

- **Тщательно продумайте, кто будет создавать файл или папку, кто будет владеть ими/администрировать их и кто будет иметь к ним доступ. Если краткосрочные консультанты создают и администрируют файлы, существует риск того, что файлы или доступ к ним останутся у консультантов, когда те уйдут!**
  - Предоставляйте доступ только тем, кому нужен файл.
  - Конфиденциальная, личная или позволяющая идентифицировать личность информация (PII) должна всегда иметь ограниченный доступ. Если вы не можете определить, следует ли ограничивать контент и каким образом, обратитесь за помощью в юридический отдел или в отдел защиты данных и конфиденциальности.

› Используйте соответствующий уровень разрешений.

- Рассмотрим пример, когда необходимо создать новый проектный документ. В большинстве случаев полный доступ должен быть только у команды, отвечающей за создание проектного документа. Когда придет время получать мнения от других коллег, предоставьте дополнительные разрешения, которые разрешают только просмотр или комментирование.
- Будьте предельно осторожны при предоставлении запросов на доступ членам команды, которые могут случайно использовать свои личные учетные записи электронной почты. Вместо предоставления доступа к личной учетной записи электронной почты предоставьте доступ к их учетной записи Mercy Corps и попросите члена команды войти в систему с этими учетными данными.

› Разрешения меняются со временем

- Если вы работаете с кем-то только в течение короткого периода времени или с людьми, не являющимися сотрудниками Mercy Corps, рассмотрите возможность предоставления временных разрешений. Если вы забудете удалить доступ позже, срок действия разрешения гарантирует, что их доступ будет приостановлен в нужное время.
- Периодически проверяйте список тех, кто имеет доступ к вашим файлам, папкам или общим дискам, чтобы убедиться, что вы удалили доступ для членов команды, которые изменили должность или больше не работают в Mercy Corps.

› Подверженный риску контент требует дополнительных действий

- Персональные данные, позволяющие идентифицировать личность (PII), данные, позволяющие идентифицировать демографические признаки или другие типы персональных данных защищены несколькими законами о защите данных. Прежде чем делиться персональными данными, проверьте юридические требования для передачи этой информации другим лицам. Неправомерный обмен персональными данными может подвергнуть риску участников программы, доноров, партнеров и членов команды Mercy Corps. Если у вас есть вопросы о персональных данных или законах о защите данных, напишите в отдел защиты данных и конфиденциальности по адресу dataprotection@mercycorps.org.
- Если информация считается конфиденциальной или служебной, делитесь ею только с необходимыми лицами и рассмотрите возможность предоставления временного доступа.
- Если лицо, получающее файл, работает в небезопасном месте или если содержимое этого файла включает персональные данные, рассмотрите возможность шифрования файла или защиты его паролем. Примеры того, как это сделать, см. в разделах «Шифрование» и «Деидентификация».

› Никогда не перемещайте файлы без разрешения владельца.

- Перемещение файлов может изменить возможность доступа к ним и сделать невозможным для других найти файл! Всегда консультируйтесь с владельцем документа, прежде чем перемещать общий файл в новое место.

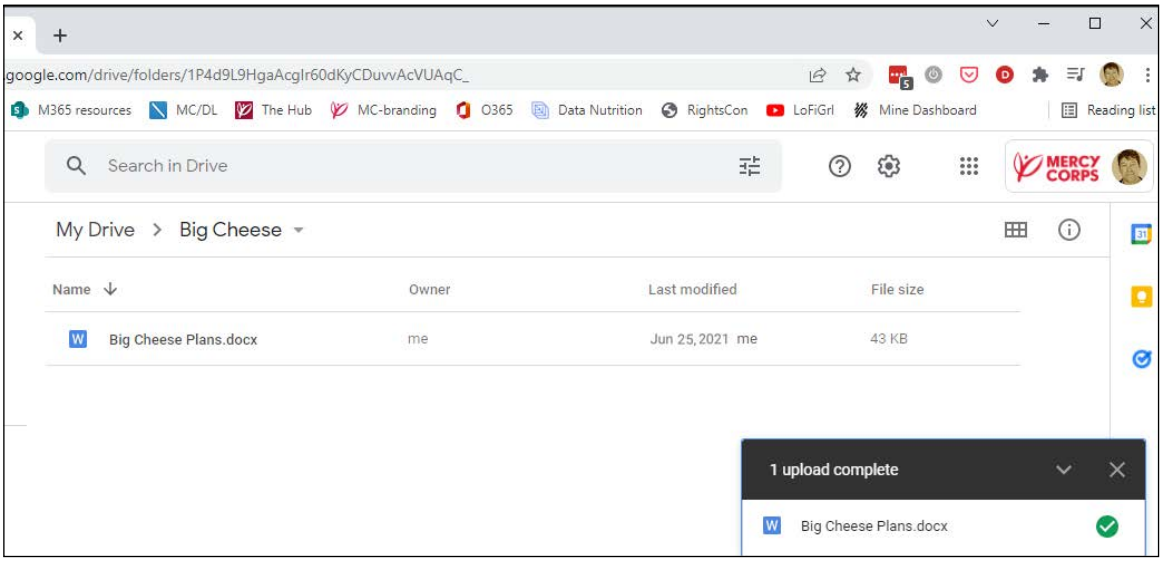
Совместное использование файлов: GDrive

Вот пример совместного использования файла с применением лучших практик на Google Диске (Google Drive). Представьте, что сейчас 2020 год, и Mercy Corps работает с консультантом (PNW Rocks) над созданием материалов для новой крупной инициативы Mercy Corps под кодовым названием Big Cheese. О проекте Big Cheese не будет объявлено публично до июля 2021 года, поэтому важно ограничить круг лиц, имеющих доступ к файлу. Для начала нам нужно совместно поработать над следующими шагами проекта в файле под названием «Big Cheese Plans».

Инструкции

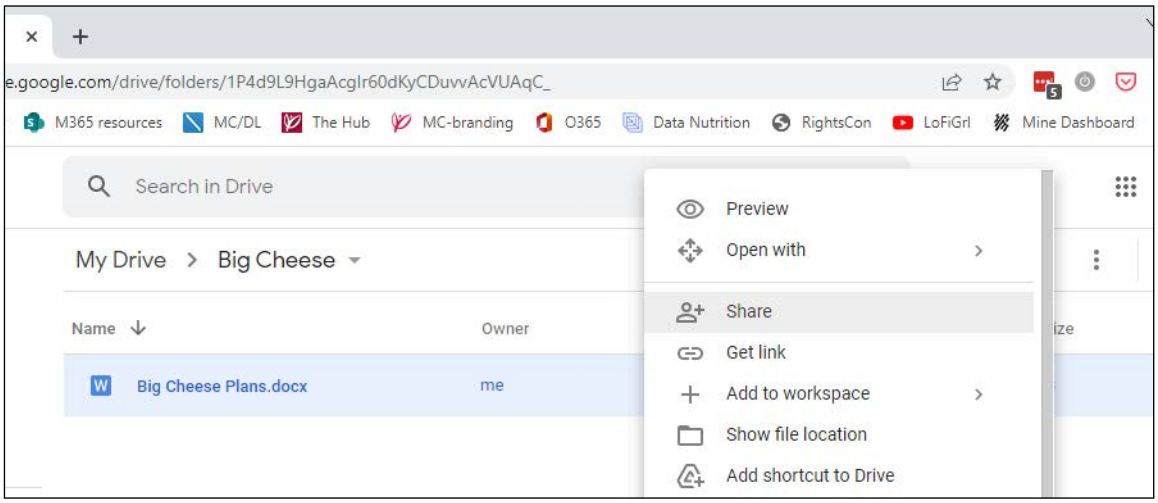
Шаг 1. Загрузить

Загрузите файл на Мой диск (My Drive).



Шаг 2. Поделиться

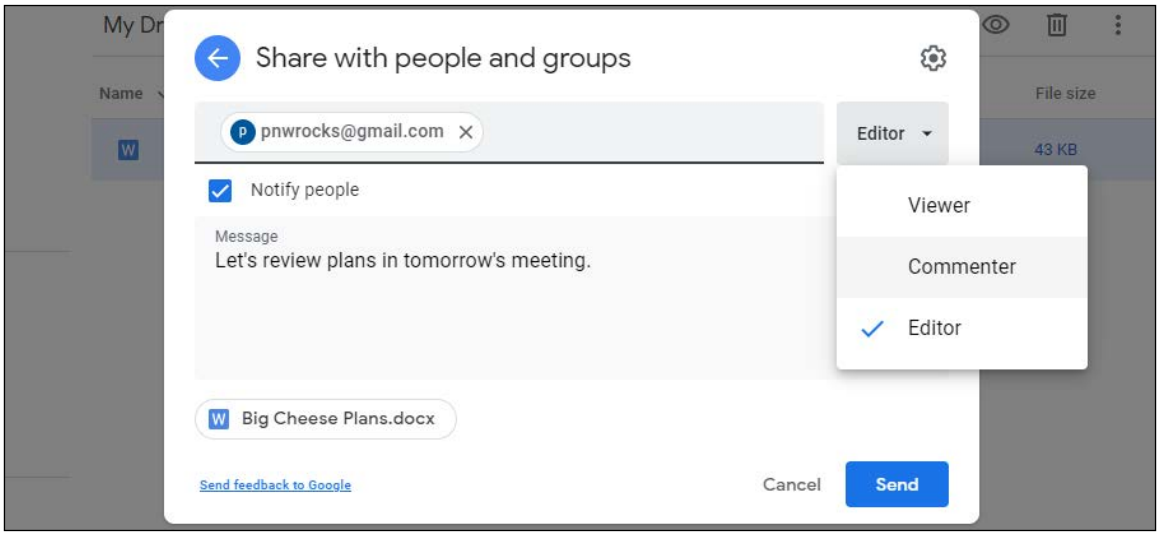
Чтобы поделиться файлом, щелкните на нем правой кнопкой мыши и выберите **Поделиться**.



- Предоставляйте доступ только тем, кому нужен файл. Когда вы делитесь файлом в разделе "Мой диск» (My Drive), по умолчанию установлено значение **Ограничено** (для отдельных лиц или групп), что является наилучшей опцией. Помните, что конфиденциальная и личная информация, а также персональные данные, позволяющие идентифицировать личность (PII) должны всегда иметь ограниченный доступ!
- Параметр **Все, у кого есть ссылка** следует использовать только для тех файлов, которые не содержат конфиденциальной информации и являются общедоступными. Если параметр **Все, у кого есть ссылка** используется для файла с конфиденциальными, персональными или финансовыми данными, он может быть легко и даже случайно опубликован, что подвергнет Mercy Corps немедленному юридическому риску, а злоумышленники легко смогут использовать информацию в преступных целях.

Шаг 3. Выберите уровень доступа

Введите адрес электронной почты человека, с которым вы хотите поделиться, затем выберите уровень доступа. По умолчанию Google использует доступ **Редактор**, который подходит только для членов рабочей группы, которым необходим полный доступ к документу. При привлечении заинтересованных сторон для получения их мнений выберите **Читатель** или **Комментатор**. Лучше всего уведомить человека и добавить сообщение, объясняющее, почему вы поделились файлом. Для отправки уведомлений оставьте флажок в пункте **Уведомлять людей**. После внесения изменений нажмите **Отправить**.

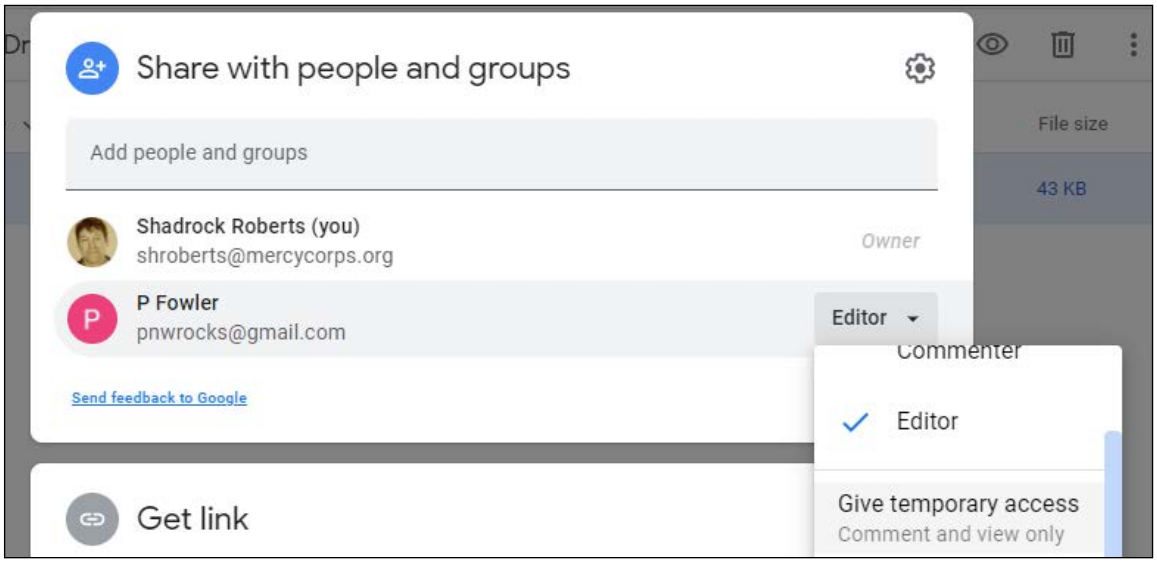


Другой вариант — отправить отдельное электронное письмо со ссылкой на файл. Для отправки уведомлений отдельно по электронной почте, снимите флажок с пункта **Уведомлять людей**. Нажав **Готово**, щелкните файл правой кнопкой мыши и выберите **Получить ссылку**. В новом всплывающем окне нажмите **Копировать ссылку** и вставьте ее в сообщение электронной почты.

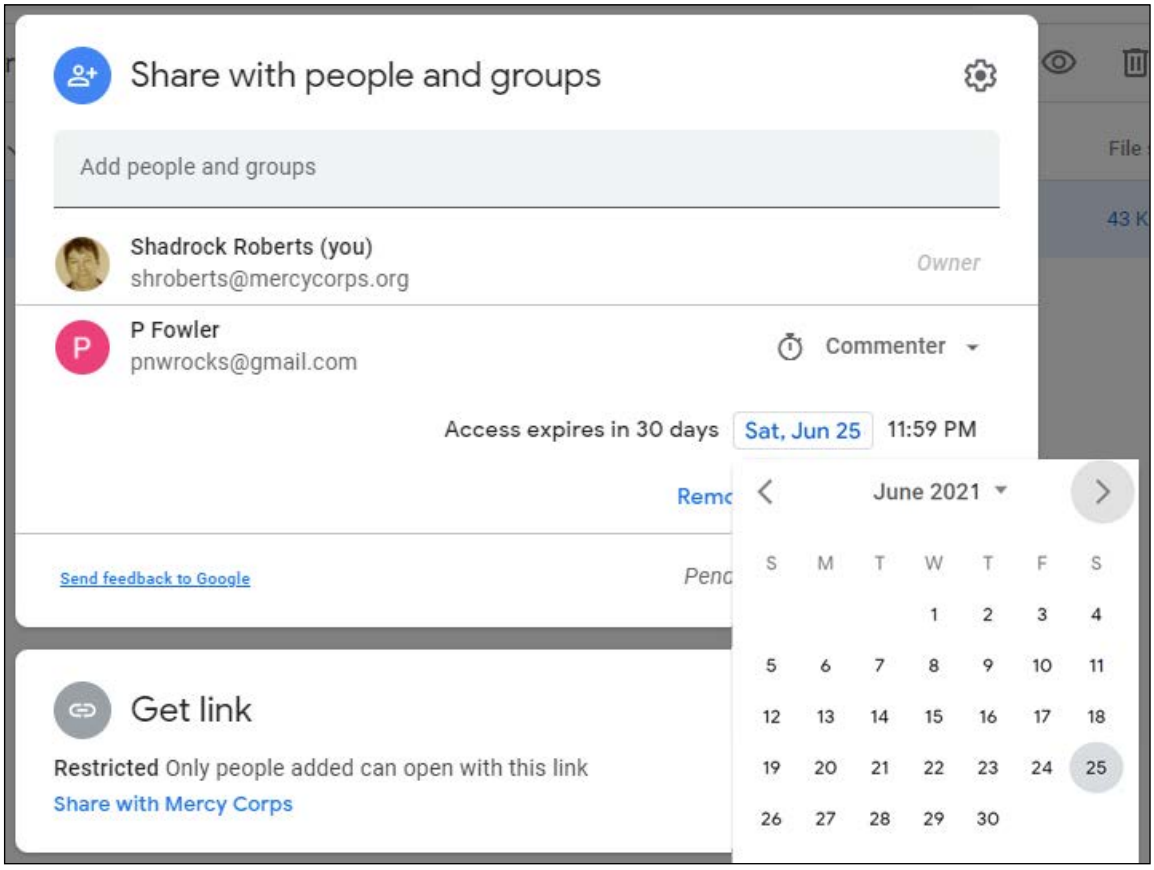
- Чтобы узнать больше об уровнях доступа, посетите страницу Общий доступ и совместная работа в «Моем диске» (My Drive).
- Если вы ограничите файл, а кто-то, у кого есть доступ, поделится ссылкой с другим человеком, этот человек не получит автоматического доступа к этому содержимому на Google Диске (Google Drive). Вместо этого они увидят веб-страницу с возможностью запросить доступ. Запрос на доступ будет отправлен владельцу файла. Запросы на доступ должны быть рассмотрены, и те, кто их получает, не должны давать разрешение на любой запрос просто так, без рассмотрения вышеприведенных примечаний и обстоятельств.

Шаг 4. Временный доступ

После того, как разрешение было предоставлено, период времени совместного использования может быть сокращен. Чтобы ограничить доступ, снова щелкните файл правой кнопкой мыши и выберите **Поделиться**. Найдите адрес электронной почты, с которым вы только что поделились, и щелкните правой кнопкой мыши на уровне доступа. Вы увидите, что появились новые опции; выберите **Предоставить временный доступ**.



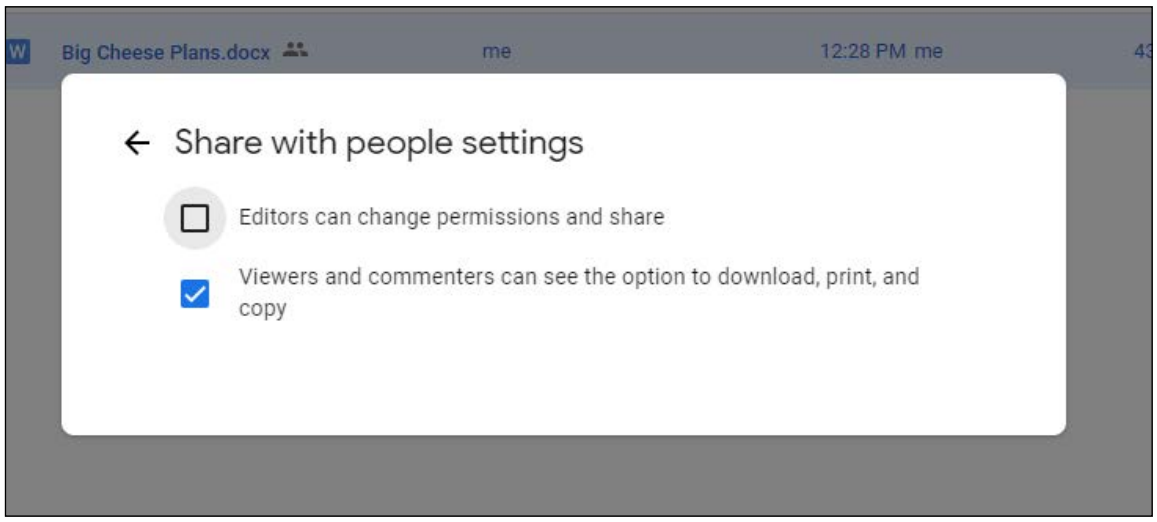
Появится календарь. Перейдите к месяцу, когда срок действия доступа должен истечь, и щелкните на соответствующей дате.



Календарь исчезнет, а отображаемая дата изменится. Вы сразу увидите, что срок действия доступа истекает в необходимую дату. Нажмите **Сохранить**.

Шаг 5. Дополнительные опции

Если у вас есть опасения по поводу того, что другие пользователи совершают ненадлежащие действия с контентом, на экране настроек доступны дополнительные опции. Доступ к настройкам файла можно получить с помощью значка шестеренки в правом верхнем углу окна обмена. Нажмите на шестеренку, и вы увидите варианты, позволяющие ограничить дальнейший обмен или отключить возможность скачивания, печати или копирования. Для любой функции, которую вы хотите отключить, просто снимите флажок. Файл быстро обновится, сохранив новую настройку.



❱ Чтобы узнать больше, посетите страницу Ограничение параметров совместного доступа на Диске (Drive).

Дополнительные рекомендации

- Не помещайте конфиденциальные файлы в папки, к которым есть общий доступ. Разрешения на папки совместного доступа распространяются на каждый файл и вложенную папку, поэтому к вашему конфиденциальному файлу может получить доступ любой, у кого есть разрешение на основную папку! Вместо этого переместите свой конфиденциальный файл в новое место за пределами более крупной структуры папок совместного доступа.
- После предоставления совместного доступа к файлу у вас есть возможность **Копировать** и/или **Переместить** файл в другое место. Никогда не перемещайте файл без разрешения владельца!
- Если вам нужно просмотреть файл на Моём диске (My Drive) или в другом месте, лучше всего использовать параметр Добавить ярлык на Диск (Drive).
- Если создается копия файла или файл перемещается, имейте в виду, что он не будет иметь тех же разрешений, что и исходный файл, если только вы намеренно не установите эти разрешения.

В этом руководстве не рассматривается совместное использование файлов на дисках Google совместного доступа или на внешних платформах для совместного использования файлов. Чтобы узнать об этом больше, посетите страницу Google Рекомендации по использованию дисков совместного доступа или управление общими дисками. Каждая из этих страниц доступна на разных языках: прокрутите страницу вниз, чтобы выбрать язык.

Лучший способ контролировать доступ к файлам с помощью Диска (Drive) — это создать группу Google и назначить разрешения участникам группы. Группы Google предназначены не только для отправки электронных писем; группы — это мощные и удобные инструменты для управления правами доступа к папкам и файлам. Подробнее о группах Google.

Если для вашего проекта требуется использование приложений за пределами G Suite, предложите своей команде загрузить Google Диск (Google Drive) для рабочего стола. Эта программа позволяет вам просматривать любые документы в разделе «Мой диск» (My Drive) или «Диски совместного доступа» (Shared drives), как если бы они были на вашем ноутбуке, даже в автономном режиме, и без необходимости загружать элемент или преобразовывать его в формат Google.

Дальнейшая помощь

То, как и с кем вы будете обмениваться данными, должно быть частью более широкой стратегии жизненного цикла данных программы или мероприятия. Есть несколько ресурсов, которые могут быть вам полезны.

- Методичка по использованию данных (Data Playbook) Международной Федерации обществ Красного Креста и Красного Полумесяца (IFRC) — это отличный источник упражнений, планов занятий, контрольных списков и других материалов, которые помогут вам организовать дискуссии и мероприятия с вашей командой на тему ответственного обращения с данными. В частности, будет полезно начать с Модуля 7 – Совместное использование данных.
- Руководство по защите данных в гуманитарной деятельности Международного комитета Красного Креста представляет собой подробное руководство практически по всем аспектам гуманитарных данных. В главе 2 конкретно рассматривается обмен данными.
- Инструментарий по ответственному обращению с данными от Партнерства по обучению обращения с наличными деньгами (Cash Learning Partnership) разработан непосредственно для специалистов, работающих с наличными и ваучерами и является золотым стандартом в руководстве по ответственным данным. В частности, см. Список подсказок #6, “Обмен данными”. Инструментарий доступен на английском, арабском, французском и испанском языках.

Обезличивание (деидентификация) данных

В этом руководстве приведен пример удаления из набора данных информации, позволяющей установить личность (PII). Существует несколько способов «деидентификации» данных, которые относятся к действиям или методам обработки, помогающим предотвратить идентификацию личности Субъекта данных. Двумя распространенными типами деидентификации являются «Анонимизация» и «Псевдонимизация».

Анонимизация — процесс, посредством которого персональные данные становятся анонимными, а человек (или «субъект данных») больше не может быть идентифицирован: это постоянное изменение данных. Распространенные методы включают в себя удаление информации, позволяющей установить личность, или шифрование значений в определенных наборах PII.

> Пример: представьте, что у организации есть данные опроса, которые содержат такие поля, как имя, государственный идентификационный код, название населенного пункта, этническая принадлежность, возраст, уровень образования и показатели здоровья. В этом случае удаление имени и государственного идентификационного кода будет первым шагом к обеспечению анонимности данных, поскольку эти «непосредственные характеристики» являются личными данными, которые прямо идентифицируют человека. Останутся «косвенные характеристики», такие как название населенного пункта, этническая принадлежность, возраст, уровень образования, показатели здоровья.

Однако даже если некоторые характеристики кажутся «анонимными», они могут таковыми не быть. Если бы опрос проводился в очень маленькой деревне, где только два жителя имеют определенную этническую принадлежность, и при этом они разного возраста, то использование этих двух косвенных характеристик могло бы позволить идентифицировать этих людей! Процесс, в ходе которого проверяются все характеристики для снижения риска повторной идентификации субъекта данных, называется Статистическим контролем раскрытия информации. Первым шагом в этом процессе является оценка риска раскрытия информации, и в Центре гуманитарных данных есть учебное онлайн-руководство по проведению оценки риска раскрытия информации.

Псевдонимизация, с другой стороны, подразумевает обработку персональных данных, после которой более невозможно установить принадлежность персональных данных конкретному субъекту данных без использования дополнительной информации, такой как код ключа.

> Пример: представьте, что опрос содержит ваше имя, адрес электронной почты, возраст, национальность и место работы. Псевдонимизация берет данные, которые можно идентифицировать конкретно о вас (ваше имя, адрес электронной почты, возраст), и делает их недоступными и отделенными от неидентифицирующих данных, таких как ваша национальность. Псевдонимные данные можно в какой-то момент восстановить, чтобы всю информацию можно было связать с конкретным источником или человеком. Вот почему псевдонимизация требует, чтобы дополнительная информация хранилась отдельно, и были приняты технические и организационные меры, обеспечивающие невозможность установления взаимосвязи указанных данных с субъектом данных.

Что выбрать: анонимизацию или псевдонимизацию?

Анонимизация, как правило, более безопасна и снижает риск раскрытия PII. Однако иногда этот процесс может слишком обобщать данные, что может сделать их бесполезными для таких программ, как оказание помощи денежными ваучерами. Если говорить о программах здравоохранения, которые включают в себя вакцинацию или другие процедуры, то может возникнуть потребность связаться с человеком для обсуждения последующего лечения. В обоих этих случаях псевдонимизация была бы лучшим вариантом, поскольку вы всегда можете восстановить целостность данных, чтобы идентифицировать человека, когда это необходимо.

Нет единого правильного ответа о том, когда лучше выбрать тот или иной метод. Прежде чем выбрать способ деидентификации ваших данных, важно понять, почему данные были собраны, осознать потенциальные риски, связанные с хранением этих данных, а также требования программы.

Также важно понимать, что методы, используемые как для анонимизации данных, так и для взлома данных, становятся все более изощренными и что даже обезличенные данные не всегда защищены на сто процентов. В случае сомнений обратитесь за помощью к своей команде по обработке данных или IT-команде.

☆ Важность

Недавние утечки данных в Международном комитете Красного Креста, взломы электронной почты в Агентстве США по международному развитию и неправильный обмен данными со стороны Верховного комиссара ООН по делам беженцев указывают на несколько путей, через которые гуманитарные данные подвергаются риску. Данные опросов домохозяйств, оценки потребностей и другие формы микроданных составляют все более значительный объем информации в гуманитарном секторе. Эти типы данных имеют решающее значение для определения потребностей и перспектив участников программы и сообществ, в которых мы работаем, но эти данные также представляют риски. Понимание того, как оценивать и управлять конфиденциальностью этих данных, абсолютно необходимо для обеспечения их безопасного, этичного и эффективного использования в различных контекстах реагирования.

Среди преимуществ использования анонимных данных по сравнению с личными данными - следующие:

- защита от неправомерного раскрытия персональных данных;
- к анонимным данным применяется меньше юридических ограничений; и
- это позволяет организациям создавать открытые или общедоступные данные, соблюдая при этом свои обязательства по защите данных.

Принципы

Обезличивание и обработка персональных данных, осуществляемая гуманитарными организациями, должна соответствовать следующим принципам.

- **Справедливость и законность обработки:** методы должны соответствовать региональному, национальному или местному законодательству или политикам, которые могут ограничивать тип данных, подходящих для обезличиания, и возможности использования определенных технологий. Любая обработка персональных данных должна быть прозрачной для вовлеченных субъектов данных.
- **Ограничение цели:** гуманитарные организации должны определить и указать конкретные цели, для которых обрабатываются данные. Эти цели должны быть явными и законными.
- **Соразмерность:** гарантия, что каждое конкретное действие, связанное с обработкой персональных данных, соответствует заявленной цели. Например: собирается ли только минимально необходимый объем данных? Принимаются ли соответствующие технические и организационные меры для снижения рисков, связанных с обработкой данных?
- **Технологические изменения:** новые наборы данных и новые инструменты для их анализа быстро меняются и совершенствуются, как и средства взлома или кражи данных. Важно понимать новые и возникающие риски для ваших данных и непрерывно корректировать свои методы и практики соответствующим образом.

Псевдонимизация

Это пример одного из способов деидентификации данных в электронной таблице. Существует множество способов деидентификации, и в этом примере используется «код ключа» для удаления личной информации, содержащейся в прямых идентификаторах, и сохранения ее в отдельном файле. Персональные данные, позволяющие идентифицировать личность (PII) — это информация, которая может быть использована для установления личности человека. Типичными примерами являются имя, адрес, номер телефона, дата рождения и номер социального страхования или государственный идентификационный код.

Инструкции

Вы можете следовать этим Инструкциям по псевдонимизации, чтобы пошагово рассмотреть базовый пример псевдонимизации набора данных. В упражнении используется демонстрационный набор данных, который находится в папке данных онлайн-руководства.

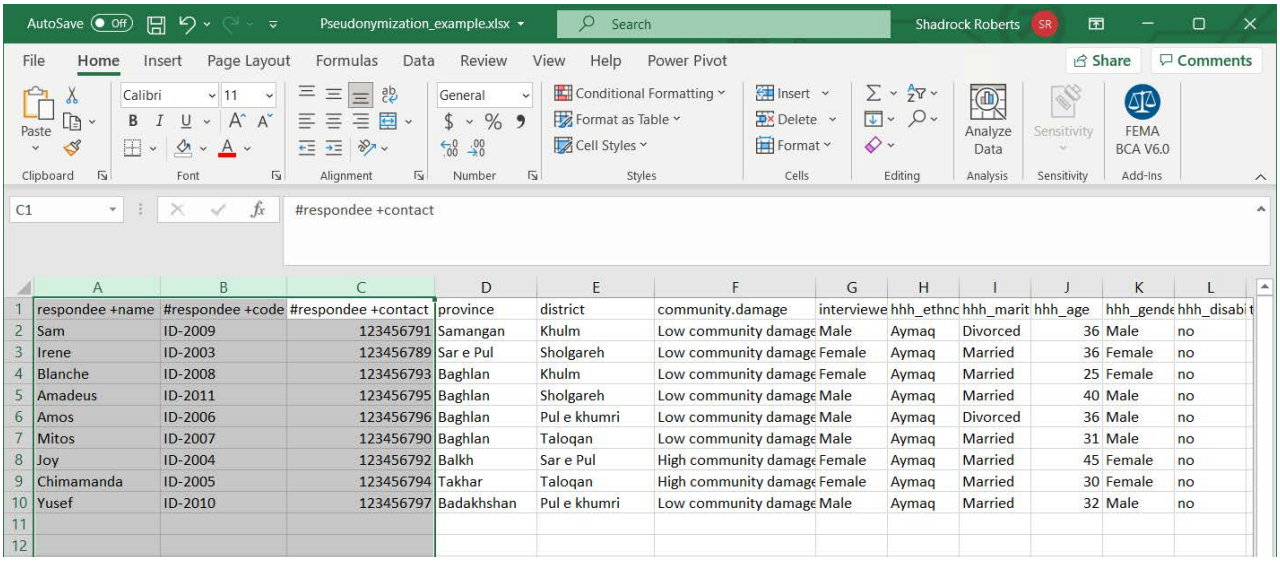
После псевдонимизации демонстрационного набора данных вы можете продолжить работу с учебным пособием Центра гуманитарных данных для проведения оценки риска раскрытия информации.

Шаг 1. Определите PII

Начните с идентификации PII в данных. В идеале у вас должны быть метаданные — данные или документ, определяющий ваши данные, — чтобы помочь вам понять, какие поля содержат PII. В демонстрационных данных есть три столбца, которые содержат потенциальные PII:

- **#респондент +имя** - содержит имя.
- **#респондент +код** - вероятно, содержит какой-либо идентификационный код.
- **#респондент +контакт** - возможно содержит номер мобильного телефона

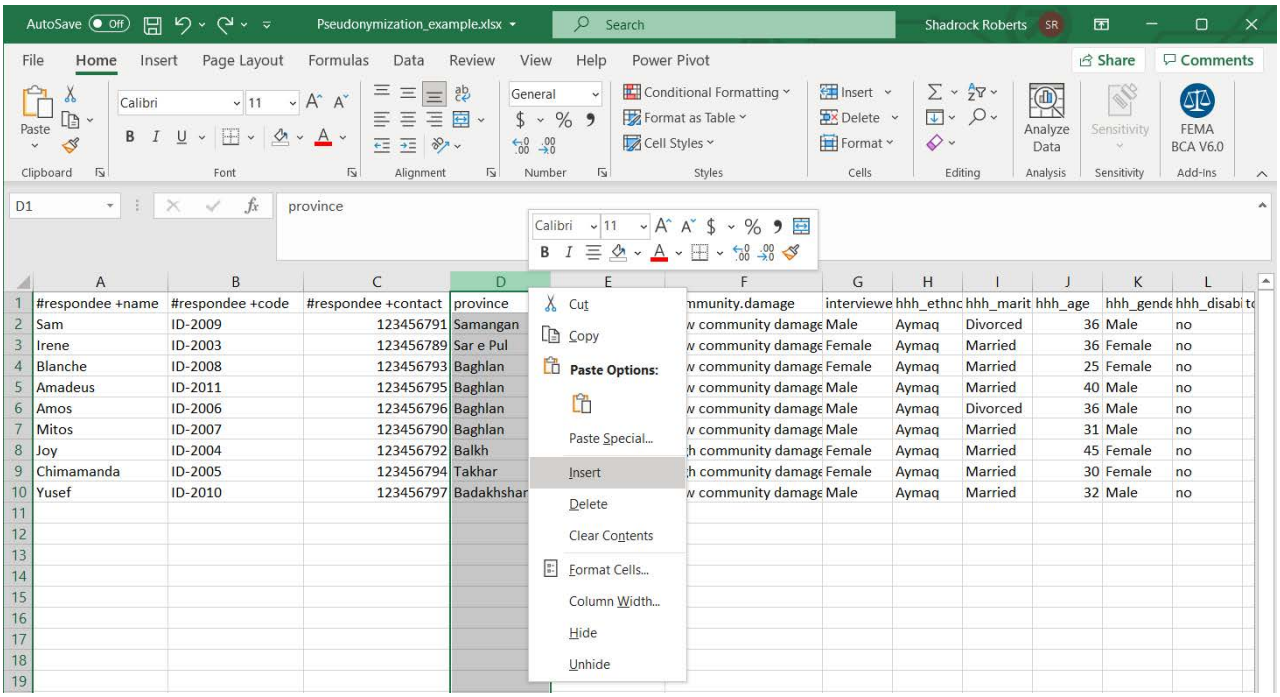
Каждый из этих прямых идентификаторов использует Гуманитарный язык обмена для маркировки данных.



	A	B	C	D	E	F	G	H	I	J	K	L
1	respondee +name	#respondee +code	#respondee +contact	province	district	community.damage	interviewe	hhh_ethnc	hhh_marit	hhh_age	hhh_gende	hhh_disabi
2	Sam	ID-2009	123456791	Samangan	Khulm	Low community damage	Male	Aymaq	Divorced	36	Male	no
3	Irene	ID-2003	123456789	Sar e Pul	Sholgareh	Low community damage	Female	Aymaq	Married	36	Female	no
4	Blanche	ID-2008	123456793	Baghlan	Khulm	Low community damage	Female	Aymaq	Married	25	Female	no
5	Amadeus	ID-2011	123456795	Baghlan	Sholgareh	Low community damage	Male	Aymaq	Married	40	Male	no
6	Amos	ID-2006	123456796	Baghlan	Pul e khumri	Low community damage	Male	Aymaq	Divorced	36	Male	no
7	Mitos	ID-2007	123456790	Baghlan	Taloqan	Low community damage	Male	Aymaq	Married	31	Male	no
8	Joy	ID-2004	123456792	Balkh	Sar e Pul	High community damage	Female	Aymaq	Married	45	Female	no
9	Chimamanda	ID-2005	123456794	Takhar	Taloqan	High community damage	Female	Aymaq	Married	30	Female	no
10	Yusef	ID-2010	123456797	Badakhshan	Pul e khumri	Low community damage	Male	Aymaq	Married	32	Male	no
11												
12												

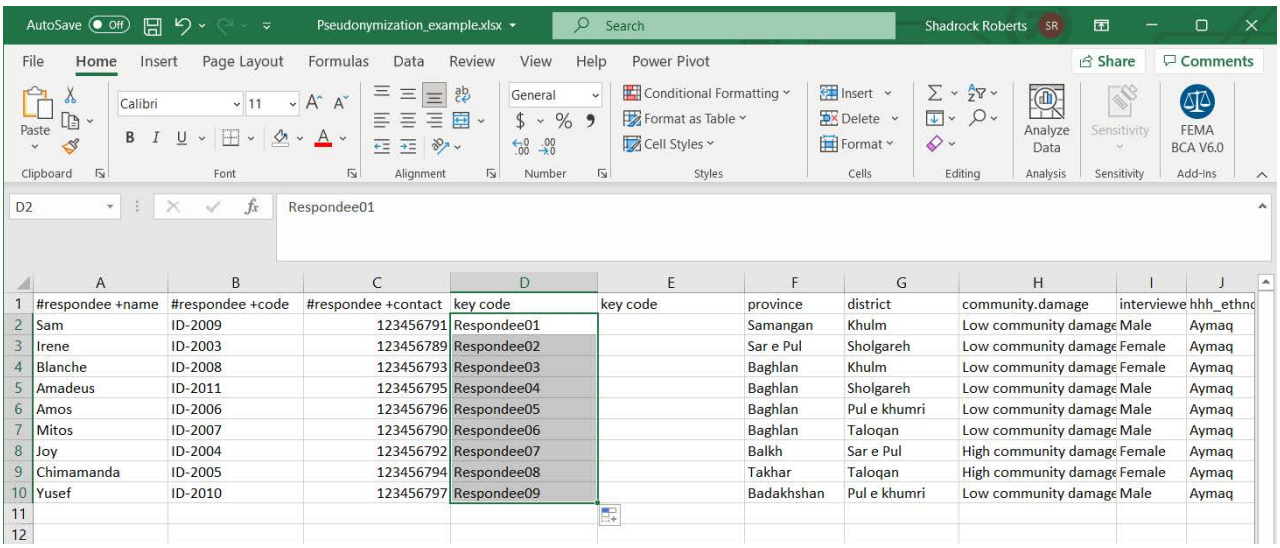
Шаг 2. Создайте новые столбцы для кода ключа

Мы будем использовать код ключа, значение, которого мы сгенерируем, чтобы раскрыть PII. Поскольку все прямые идентификаторы сгруппированы вместе, мы создадим два новых столбца между столбцами C, **#респондент +контакт** и D, **область**. В Excel мы делаем это, выделяя столбец справа от того места, куда мы хотим вставить новые столбцы, щелкаем правой кнопкой мыши на столбце и выбираем **Вставить**. Повторите этот процесс еще раз, чтобы создать еще один пустой столбец.



Шаг 3 — Создайте код ключа

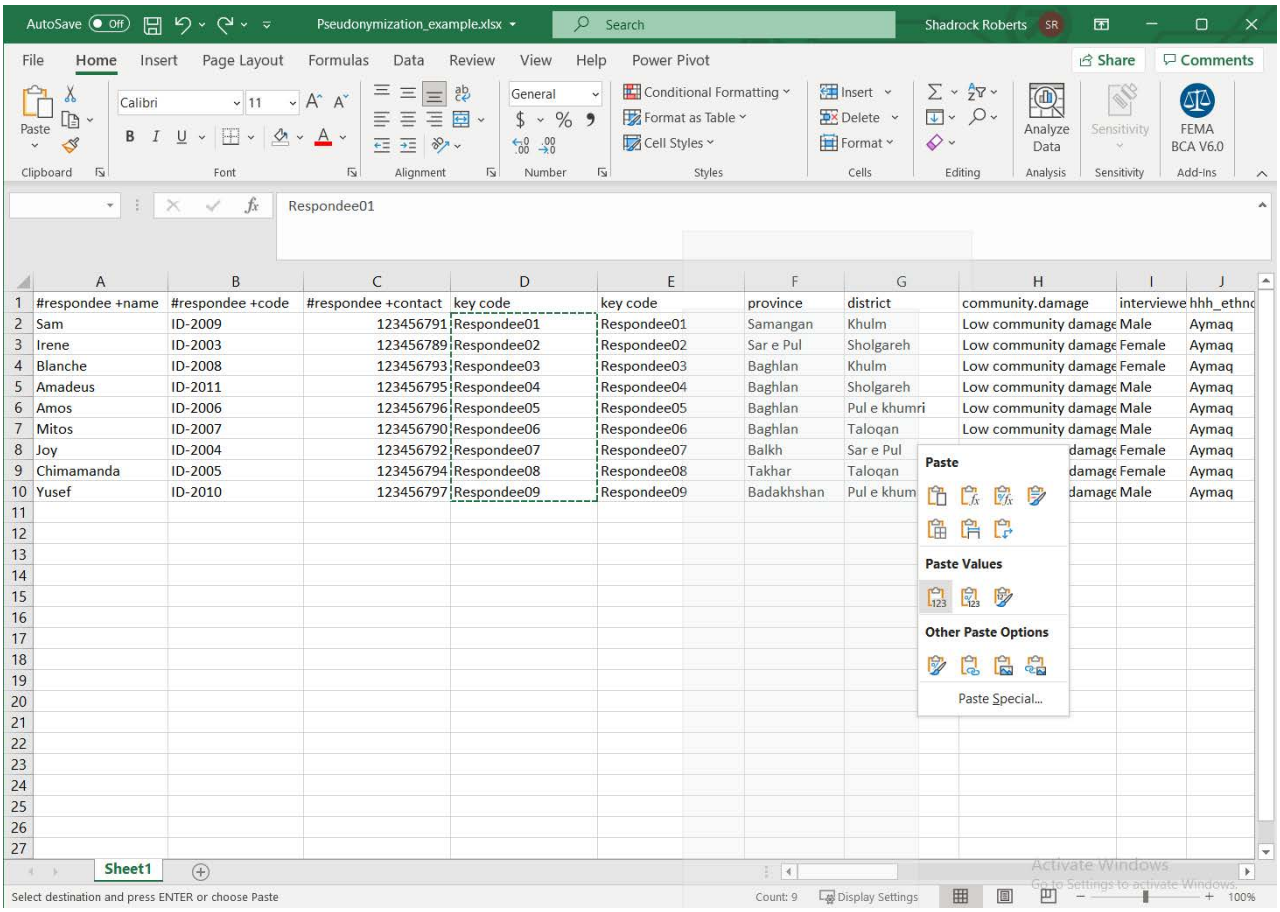
Начните с названия новых столбцов. Мы будем использовать «ключевой код» в каждом из них: каждый столбец будет содержать одинаковые значения. Сейчас самое время обновить любые метаданные об этом наборе данных, чтобы объяснить, что означает **«код ключа»** Далее мы воспользуемся функцией Excel Автозаполнение для создания простого кода. Введите **Респондент01** в первой ячейке. Затем выделите эту ячейку, щелкните указатель перемещения в правом нижнем углу ячейки и перетащите вниз до конца набора данных. Это автоматически заполнит окончательный номер каждой записи, присвоив каждому респонденту новый код.



	A	B	C	D	E	F	G	H	I	J
1	#respondee +name	#respondee +code	#respondee +contact	key code	key code	province	district	community.damage	interviewe	hhh_ethnc
2	Sam	ID-2009	123456791	Respondee01		Samangan	Khulm	Low community damage	Male	Aymaq
3	Irene	ID-2003	123456789	Respondee02		Sar e Pul	Sholgareh	Low community damage	Female	Aymaq
4	Blanche	ID-2008	123456793	Respondee03		Baghlan	Khulm	Low community damage	Female	Aymaq
5	Amadeus	ID-2011	123456795	Respondee04		Baghlan	Sholgareh	Low community damage	Male	Aymaq
6	Amos	ID-2006	123456796	Respondee05		Baghlan	Pul e khumri	Low community damage	Male	Aymaq
7	Mitos	ID-2007	123456790	Respondee06		Baghlan	Taloqan	Low community damage	Male	Aymaq
8	Joy	ID-2004	123456792	Respondee07		Balkh	Sar e Pul	High community damage	Female	Aymaq
9	Chimamanda	ID-2005	123456794	Respondee08		Takhar	Taloqan	High community damage	Female	Aymaq
10	Yusef	ID-2010	123456797	Respondee09		Badakhshan	Pul e khumri	Low community damage	Male	Aymaq
11										
12										

Шаг 4. Продублируйте код ключа и удалите формулы

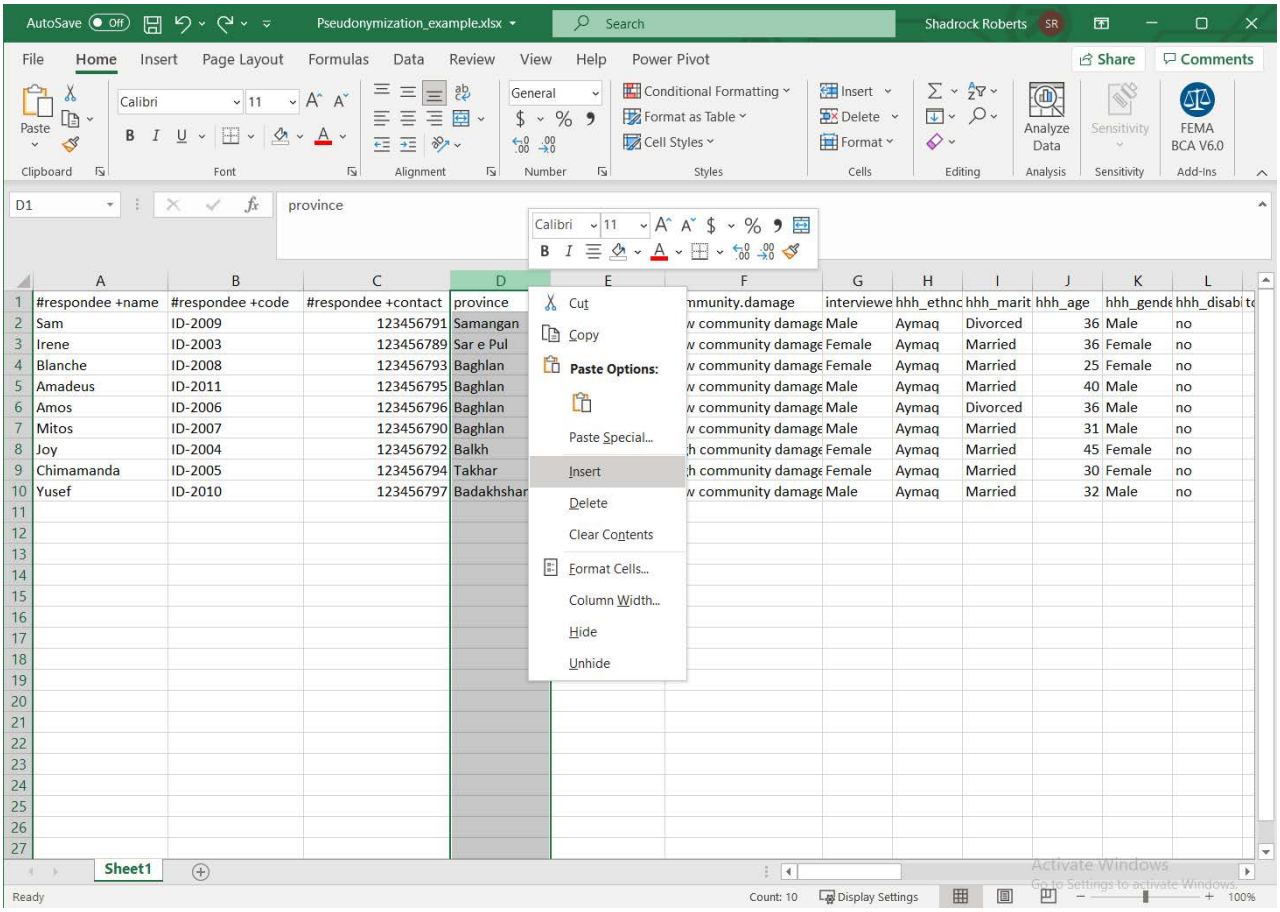
Теперь мы скопируем код ключа и вставим его в соседний столбец. Это можно сделать с помощью основных клавиатурных команд, таких как **ctrl + C** или выделить ячейки, которые нужно скопировать, щелкнуть по ним правой кнопкой мыши и выбрать **Копировать**. В соседнем столбце выделите ячейки, в которые вы хотите вставить новый код ключа, щелкните правой кнопкой мыши и выберите **Вставить**. Мы специально выбрали вставить только значения. Если вы использовали формулу для создания нового кода, важно сохранить только значения для использования в качестве кода ключа!



	A	B	C	D	E	F	G	H	I	J
1	#respondee +name	#respondee +code	#respondee +contact	key code	key code	province	district	community.damage	interviewe	hhh_ethn
2	Sam	ID-2009	123456791	Respondee01	Respondee01	Samangan	Khulm	Low community damage	Male	Aymaq
3	Irene	ID-2003	123456789	Respondee02	Respondee02	Sar e Pul	Sholgareh	Low community damage	Female	Aymaq
4	Blanche	ID-2008	123456793	Respondee03	Respondee03	Baghlan	Khulm	Low community damage	Female	Aymaq
5	Amadeus	ID-2011	123456795	Respondee04	Respondee04	Baghlan	Sholgareh	Low community damage	Male	Aymaq
6	Amos	ID-2006	123456796	Respondee05	Respondee05	Baghlan	Pul e khumri	Low community damage	Male	Aymaq
7	Mitos	ID-2007	123456790	Respondee06	Respondee06	Baghlan	Taloqan	Low community damage	Male	Aymaq
8	Joy	ID-2004	123456792	Respondee07	Respondee07	Balkh	Sar e Pul	damage	Female	Aymaq
9	Chimamanda	ID-2005	123456794	Respondee08	Respondee08	Takhar	Taloqan	damage	Female	Aymaq
10	Yusef	ID-2010	123456797	Respondee09	Respondee09	Badakhshan	Pul e khum	damage	Male	Aymaq

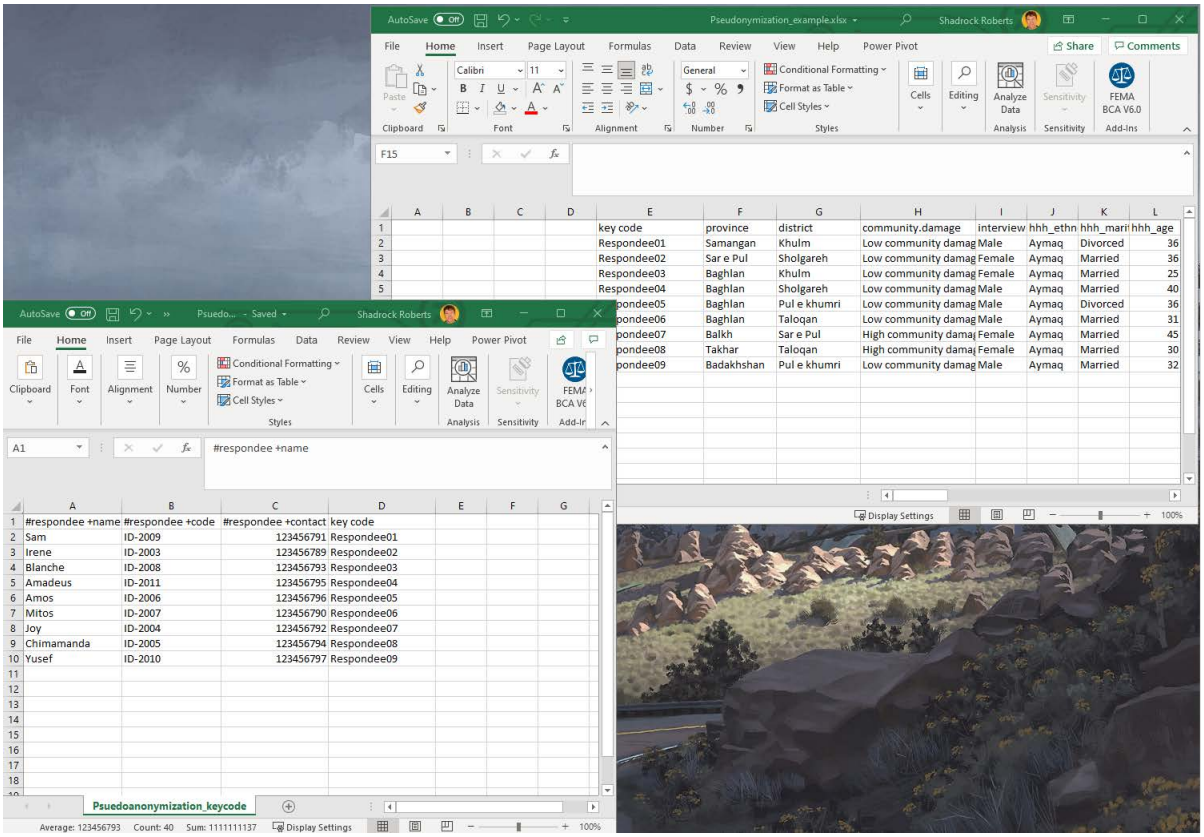
Шаг 5. Разделите прямые и косвенные идентификаторы

Выделите столбцы, содержащие прямые идентификаторы с PII, вместе с одним из столбцов кода ключа. В этом примере мы выделяем столбцы A-D. Щелкните их правой кнопкой мыши и выберите **Вырезать**.



	A	B	C	D	E	F	G	H	I	J	K	L
1	#respondee +name	#respondee +code	#respondee +contact	province		mmunity.damage	interviewe	hhh_ethnc	hhh_marit	hhh_age	hhh_gende	hhh_disabi
2	Sam	ID-2009	123456791	Samangan		w community damage	Male	Aymaq	Divorced	36	Male	no
3	Irene	ID-2003	123456789	Sar e Pul		w community damage	Female	Aymaq	Married	36	Female	no
4	Blanche	ID-2008	123456793	Baghlan		w community damage	Female	Aymaq	Married	25	Female	no
5	Amadeus	ID-2011	123456795	Baghlan		w community damage	Male	Aymaq	Married	40	Male	no
6	Amos	ID-2006	123456796	Baghlan		w community damage	Male	Aymaq	Divorced	36	Male	no
7	Mitos	ID-2007	123456790	Baghlan		w community damage	Male	Aymaq	Married	31	Male	no
8	Joy	ID-2004	123456792	Balkh		h community damage	Female	Aymaq	Married	45	Female	no
9	Chimamanda	ID-2005	123456794	Takhar		h community damage	Female	Aymaq	Married	30	Female	no
10	Yusef	ID-2010	123456797	Badakhshar		w community damage	Male	Aymaq	Married	32	Male	no

Затем откройте новую таблицу и вставьте эти значения с помощью сочетания клавиш **ctrl + V** или другим способом. Сохраните новую таблицу. Теперь у вас есть две таблицы: одна из них содержит косвенные идентификаторы, а новая таблица содержит прямые идентификаторы с PII. Оба набора данных содержат ключевой код для каждой записи в данных, чтобы при необходимости все данные можно было объединить.



Дальнейшие шаги

Оба файла содержат ключевой код, который позволит их собрать вместе. Один из способов сделать это в Excel — использовать функцию VLOOKUP для автоматического заполнения ячеек на основе значений других ячеек. В этом случае вы можете заполнить пустые ячейки исходного файла отсутствующими идентификационными данными на основе значения **ключевого кода**.

Поскольку новый файл содержит прямые идентификаторы, содержащие PII, он должен храниться в безопасном месте. Отличный способ сделать это — зашифровать файл и использовать облачное хранилище для ограничения доступа к файлу (**см. руководства по Лучшим практикам шифрования и совместного использования файлов**).

Помните: даже при том, что исходная электронная таблица была деидентифицирована путем удаления прямых идентификаторов, содержащих очевидную PII, другие косвенные идентификаторы могут быть объединены с другими данными или проанализированы таким образом, чтобы можно было идентифицировать человека.

По этой причине оба файла должны храниться в безопасном месте. Если вы хотите предоставить более широкий доступ к исходному файлу, не содержащему PII, крайне важно выполнить оценку риска раскрытия информации, чтобы обеспечить минимальный уровень риска повторной идентификации данных. В Центре гуманитарных данных есть онлайн-руководство по проведению оценки рисков раскрытия информации с использованием статистического программного обеспечения с открытым исходным кодом “R”. Кроме того, на веб-странице Poverty Action Lab Деидентификация для публикации данных содержится отличное обсуждение обезличивания данных и пример кода для статистического программного обеспечения Stata. Для внутреннего использования сотрудниками Mercy Corps доступен Проект руководства от T4D, который содержит дополнительные формулы Excel.

Наконец, все эти шаги вместе помогают снизить риски или раскрытие PII, поэтому они должны быть перечислены в PIA (**см. Руководство по оценке влияния на конфиденциальность**), чтобы другие понимали, как эти данные защищаются.

Дальнейшая помощь

Деидентификация данных является частью надлежащей практики управления данными и более широкого жизненного цикла данных, который представляет собой общие действия по сбору отдельных данных в рамках программной деятельности или реагирования. Следующие ресурсы можно использовать как эффективные отправные точки для более полного понимания ответственного управления вашими данными.

- Инструментарий ответственного использования данных от Cash Learning Partnership разработан специально для специалистов, работающих с наличными и ваучерами, и он является золотым стандартом в руководстве по ответственным данным. Инструментарий доступен на английском, арабском, французском и испанском языках.
- Стартовый комплект данных для полевого гуманитарного персонала Сообщества для активного обучения электронным денежным переводам (Electronic Cash Transfer Learning Action Network) содержит материалы для разъяснения различных аспектов надлежащего управления данными и методов защиты.
- Руководство по защите данных в гуманитарной деятельности Международного комитета Красного Креста представляет собой подробное руководство практически по всем аспектам гуманитарных данных. Глава 2 посвящена обезличиванию данных.
- Справочник современного специалиста в области развития от Engine Room — хороший обзор данных в контексте международной деятельности в области международного развития. В разделе Общий доступ к данным конкретно рассматривается деидентификация.

Шифрование файла

В этом разделе рассматривается базовый пример шифрования файла с помощью функции Microsoft, доступной на компьютерах Mercy Corps. Существует ряд факторов, которые следует учитывать при шифровании файла, но конкретно здесь мы сосредоточимся на использовании пароля и шифровании одного файла. См. приведенные ниже ссылки на ресурсы, которые более подробно раскрывают суть шифрования. Однако для этого руководства полезно понимать тонкую разницу между «защитой паролем» и «шифрованием».

Думайте о защите паролем как о коробке с замком. Когда вы «защищаете паролем» свой документ, вы кладете его в электронный ящик и запираете его паролем: только тот, у кого есть пароль, может открыть ящик. Однако, если выбранный вами пароль не очень надежный или если он предоставлен не тому человеку, кто-то может легко получить доступ к ящику и просмотреть ваш документ! Шифрование же, напротив, использует сложные алгоритмы для кодирования информации, что требует наличия ключа для расшифровки этой информации. Представляйте это так, как будто вы берете свой документ и пропускаете его через машину для измельчения бумаги, в которой есть специальная клавиша, чтобы воссоздать документ.

Когда вы сочетаете защиту паролем и шифрование, вы фактически удваиваете свою защиту. Если кто-то успешно взломает пароль к электронному ящику, он сможет увидеть только «кусочки измельченной бумаги», не имея при этом надлежащего ключа. Все ноутбуки Mercy Corps зашифрованы с помощью Microsoft BitLocker. Это предотвращает извлечение жесткого диска ноутбука Mercy Corps и доступ к нему на другом компьютере.

☆ Важность

Шифрование имеет решающее значение, поскольку оно помогает обеспечить конфиденциальность и безопасность информации. Без шифрования данные могут быть перехвачены и прочитаны любым, кто имеет к ним доступ. Рассматривая вопрос о том, следует ли шифровать данные, спросите себя: «Каков риск для участников, сотрудников и партнеров программы Mercy Corps, если эти данные будут утеряны или украдены?» Хорошее проверенное правило — шифровать все, что содержит личную или закрытую («чувствительную) информацию.

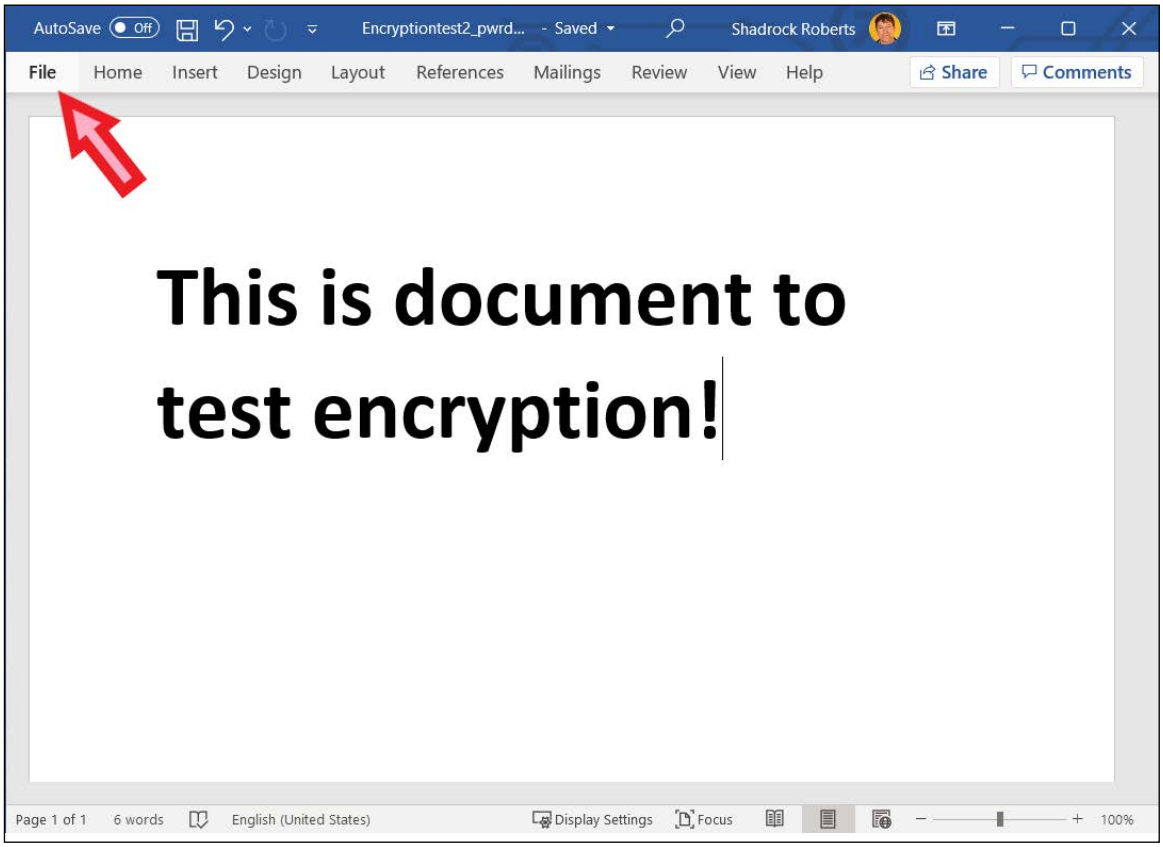
Принципы

- Используйте одобренные Mercy Corps системы для зашифрованной передачи и хранения данных (например, Microsoft SharePoint или Google Drive). Если вы сомневаетесь, обратитесь за советом к местному IT-специалисту.
- Шифруйте конфиденциальные данные на всех этапах их сбора, использования, передачи и хранения.
- Используйте надежные пароли и не используйте их повторно. Списки паролей распространяются в Интернете и упрощают доступ к нескольким вашим учетным записям или файлам для тех, у кого есть один из ваших паролей! Вы можете использовать менеджер паролей, например Lastpass. Однако менеджеры паролей могут быть уязвимы для кибератак со стороны поддельных приложений, поэтому крайне важно, чтобы менеджеры паролей использовались как часть более широкого подхода к защите данных.

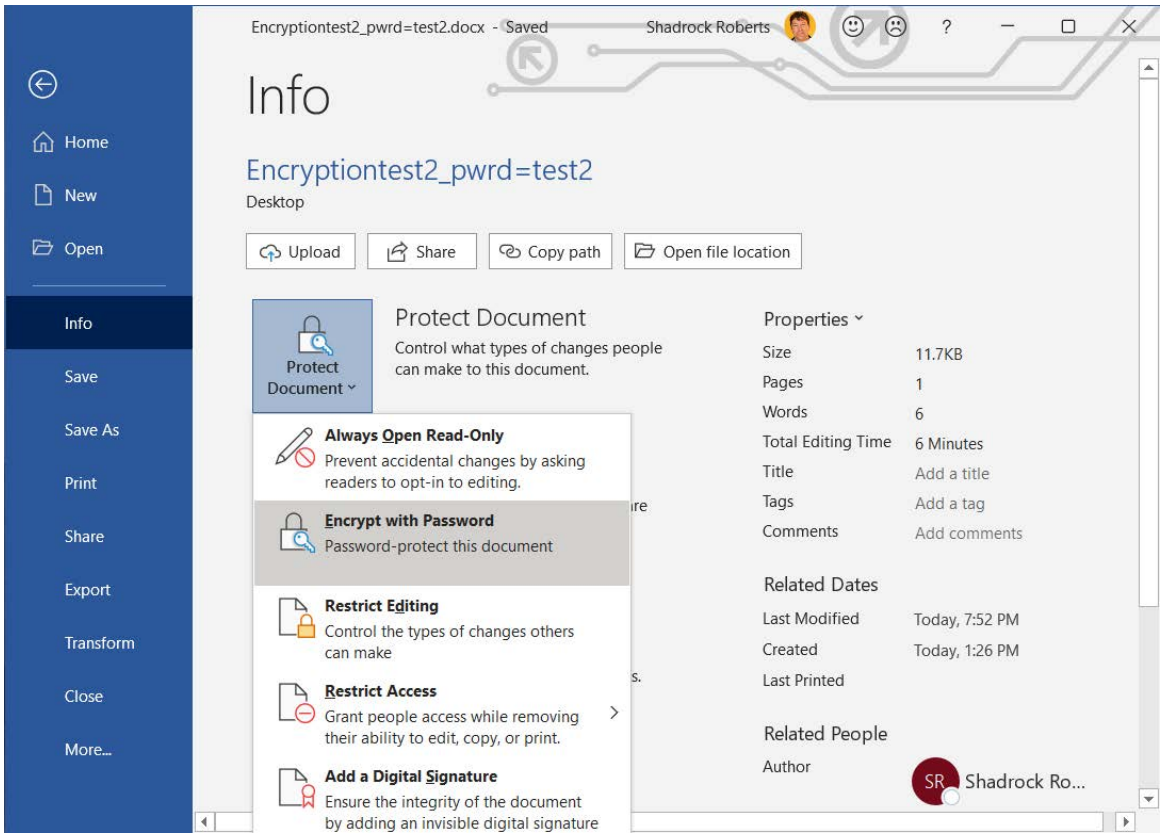
- Однако, для шифрования в командной среде не следует забывать о принципе «где тонко, там и рвется». Если хотя бы один человек не использует шифрование, данные вашей программы находятся под угрозой. Чрезвычайно важно сообщить об этом вашей команде: шифрование — это не только вопрос технологии, но и корректировки поведения.
- Изучите законы, регулирующие шифрование в вашей стране. Местные законы в ряде стран (например, в Судане, Йемене и Пакистане) накладывают ограничения на программное обеспечение для шифрования. Если вы сомневаетесь, обратитесь за советом к местному IT-специалисту: как правило, они помогают вам обеспечить надлежащее шифрование жесткого диска вашего компьютера с помощью Intune.

Инструкции

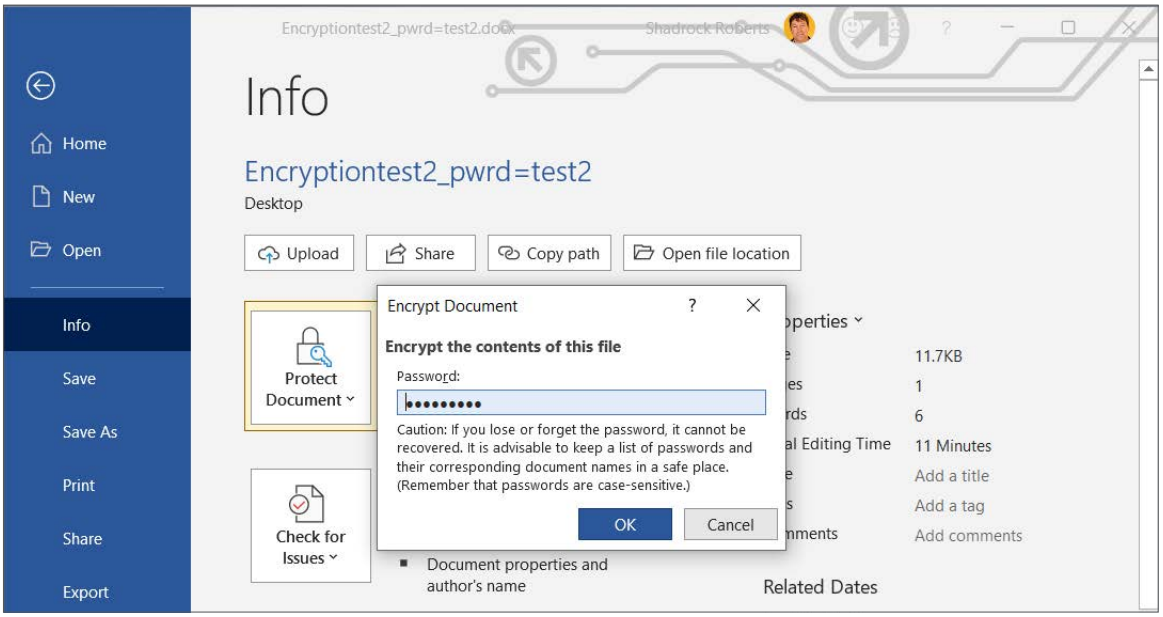
1 Откройте файл Word, Excel или PowerPoint, который нужно зашифровать, и выберите меню **Файл**.



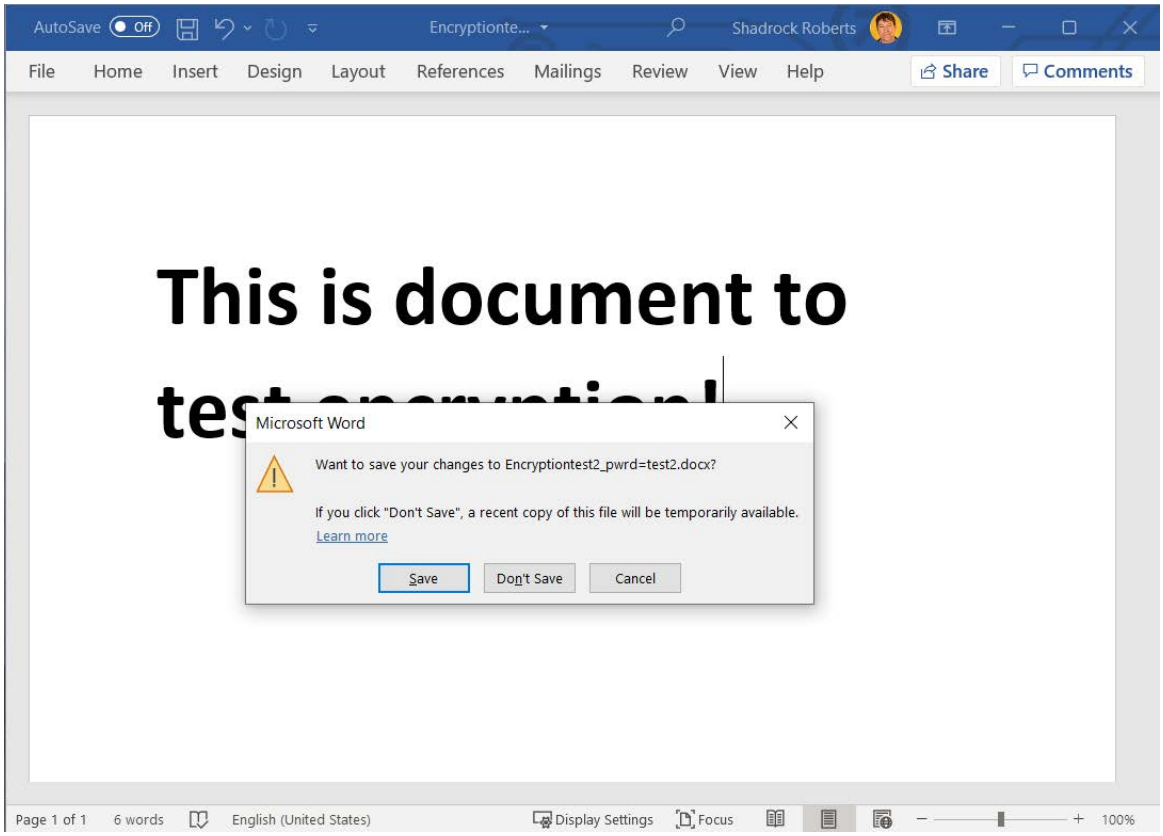
2 Перейдите к **Информация** > **Защитить документ** > **Зашифровать паролем**.



3 Введите пароль, нажмите **OK**, затем введите его еще раз для подтверждения.



4 Сохраните файл для вступления пароля в силу.



Теперь вы можете поделиться файлом и паролем с теми, кому требуется доступ. Рекомендуется поместить файл в одобренную Mercy Corps облачную службу, такую как G Suite или SharePoint. Не забудьте отправить ссылку на файл и ссылку на пароль отдельно. Например, вы можете поделиться файлом с помощью Google Диска (Google Drive) (**См.раздел «Совместное использование файлов»**) и создать уведомление о том, что файл был предоставлен через Google, а затем передать пароль по электронной почте коллеге.

Дальнейшая помощь

- Стартовый комплект данных от Electronic Cash Transfer Learning Action Network содержит список подсказок по шифрованию (см. список подсказок № 5).
- Electronic Frontier Foundation предоставляет более подробный обзор различных форм шифрования.
- Справочник современного специалиста в области развития от Engine Room, включает раздел об управлении данными, в котором приводятся дополнительные общие сведения о шифровании.

КОНТАКТЫ

ХИЗЕР ЛАВ (HEATHER LOVE)
Директор по глобальной защите данных и конфиденциальности | IT
hlove@mercycorps.org

ШЕДРОК РОБЕРТС (SHADROCK ROBERTS)
Специалист по защите данных |IT
shroberts@mercycorps.org

О Mercy Corps

Mercy Corps — ведущая международная организация, в основе работы которой лежит вера в возможность сделать этот мир лучше. В бедствиях и в трудностях, в более чем 40 странах мира мы трудимся, чтобы претворять в жизнь смелые решения , помогая людям преодолевать невзгоды и строить более сильные изнутри сообщества. Сейчас и для будущего.

MERCY CORPS

Международная штаб-квартира
45 SW Ankeny Street
Portland, Oregon 97204
888 842 0842
mercycorps.org

Европейская штаб-квартира
40 Sciences
Edinburgh EH9 1NJ
Scotland, UK
+44 131 662 5160
mercycorps.org.uk