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

ДОВІДНИКИ ІЗ ЗАХИСТУ ДАНИХ І КОНФІДЕНЦІЙНОСТІ

MERCY CORPS

Наведені нижче матеріали покликані допомогти співробітникам Mercy Corps краще зрозуміти та впровадити практики відповідального ставлення до даних. Тут зібрано кілька наявних політик і методичних документів Mercy Corps і деякі прості навчальні посібники та посилання на інші ресурси. Інформацію можна сприймати як всеосяжний довідник, або кожен розділ може бути використано як самостійний посібник із певної теми.

Хоча цей посібник призначений у першу чергу для співробітників Mercy Corps і був розроблений для доповнення "Інструментарію відповідального ставлення до даних", ми випускаємо його із відкритою ліцензією, щоби він міг принести користь партнерам, подібним до нашої організаціям і всім, хто потребує зразків політик, шаблонів та інструкцій для впровадження практик відповідального ставлення до даних. Усі наші довідкові матеріали можна завантажити на нашій сторінці Github за адресою https://github.com/mercycorps/DPP-guides.

Зміст

Список джерел

Матеріали, представлені в цьому посібнику, є частиною практик належного керування даними та більшого життєвого циклу даних або загальної діяльності з керування індивідуальними даними як складової програми або відгуку. Наступні ресурси є відмінним початком для повнішого розуміння управління вашими даними відповідальним чином. Ми використовували і цитували уривки з усіх цих ресурсів у цьому посібнику та посилаємося на конкретні глави або розділи, які найбільше стосуються певної теми.

- "Інструментарій відповідальності за дані" від Cash Learning Partnership призначений спеціально для тих, хто використовує готівку та ваучери, але є золотим стандартом настанов із відповідального ставлення до даних. Інструментарій доступний англійською, арабською, французькою й іспанською мовами.
- "Набір для початківців про дані для працівників гуманітарної сфери" від Electronic Cash Transfer Learning Action Network містить низку порад щодо даних для розуміння різних аспектів практик належного керування даними та їх захисту.
- "Довідник із захисту даних у гуманітарній діяльності" від Міжнародного Комітету Червоного Хреста є докладним посібником майже з усіх аспектів гуманітарних даних.
- "Збірник даних" від Міжнародної Федерації Товариств Червоного Хреста та Червоного Півмісяця є відмінним ресурсом вправ, планів занять, контрольних списків та інших матеріалів, які допоможуть вам організувати бесіди та заходи зі своєю командою для розробки заходів, присвячених відповідальному ставленню до даних.
- Онлайн-навчання від Центру гуманітарних даних для проведення оцінки ризику розкриття інформації є дуже специфічним, технічним ресурсом, але незамінним для справжнього зниження ризику використання даних для ідентифікації осіб.
- "Довідник спеціаліста із сучасного розвитку" від Engine Room — хороший огляд питання даних у контексті міжнародної діяльності з розвитку.

Ліцензія

Розуміння чутливих даних

Може бути складно зрозуміти різні класифікації даних, але вони є важливою частиною роботи з гуманітарними даними. Наприклад, у чому різниця між персональними даними та чутливими даними? Певні типи даних можуть вимагати особливої обережності відповідно до регіонального або національного законодавства або організаційної політики та можуть представляти різні типи ризику як для учасників програми, так і для організацій. Чутливі дані є підкатегорією персональних даних, і в цьому розділі містяться детальні вказівки щодо їх обробки та розуміння.

☆ Важливість

Більшість програм та інших заходів Mercy Corps збирають певну особисту інформацію про осіб. У багатьох випадках програми також збирають інформацію про культурний профіль людини, сексуальну орієнтацію, здоров'я або біометрію та генетику. Ці типи інформації вважаються чутливими даними, і якщо їх буде розкрито, до них отримають доступ або передадуть їх неналежним чином, результатом може стати:

- ❱ - шкода особі, зокрема санкції, дискримінація та загрози безпеці;
- ❱ - негативний вплив на здатність Mercy Corps здійснювати діяльність і зниження довіри або сприйняття громадськістю.

Життєво важливо вжити необхідних заходів для захисту цих даних.

Довідник

Цей розділ містить два документи.

- ❱ "Довідник з обробки чутливих даних" знайомить вас із чутливими даними, ключовими термінами та речами, які слід враховувати при плануванні їх збору, зберігання, аналізу та обміну ними.
  - Співробітники Mercy Corps можуть отримати доступ до посібника у внутрішній цифровій бібліотеці Mercy Corps.
  - Будь-хто може завантажити документ із посібником англійською, арабською, іспанською, французькою та російською мовами.
- ❱ "Шаблон оцінки чутливої інформації (ОЧІ)" можна використовувати разом з оцінкою впливу на конфіденційність для документування всіх додаткових гарантій, які використовуються для чутливих даних. Цей документ також визначає різні правові основи, які можуть бути використані для виправдання збору та використання чутливих даних.
  - Співробітники Mercy Corps можуть отримати доступ до шаблону ОЧІ у внутрішній цифровій бібліотеці Mercy Corps.
  - Будь-хто може завантажити документ Microsoft Word із шаблоном англійською, арабською, іспанською, французькою та російською мовами.

Додаткова підтримка

Планування збору або використання чутливих даних має бути частиною більшої стратегії для життєвого циклу даних програми або заходу. Є кілька ресурсів, які можуть вам допомогти.

- ″Збірник даних″ від Міжнародної Федерації Товариств Червоного Хреста і Червоного Півмісяця (IFRC) є відмінним ресурсом вправ, планів занять, контрольних списків та інших матеріалів, які допоможуть вам організувати бесіди та заходи зі своєю командою. Зокрема, варто почати з Модуля 4 — Відповідальне ставлення до даних.
- ″Довідник із захисту даних у гуманітарній діяльності″ від Міжнародного Комітету Червоного Хреста є докладним посібником майже з усіх аспектів гуманітарних даних. Глава 3 присвячена конкретно правовій основі обробки персональних даних.
- ″Інструментарій відповідальності за дані″ від Cash Learning Partnership призначений спеціально для тих, хто використовує готівку та ваучери, але є золотим стандартом настанов із відповідального ставлення до даних. Зокрема, на листку порад №*2* ″Розробка та план″ обговорюється законна підстава для чутливих даних. Інструментарій доступний англійською, арабською, французькою й іспанською мовами.

Оцінки впливу на конфіденційність

Цей посібник допоможе вам зрозуміти оцінку впливу на конфіденційність (ОВК) і містить настанови та шаблон ОВК, що використовуються в Mercy Corps. Шаблон ОВК містить низку запитань, що створюють основу для визначення потенційних ризиків конфіденційності, пов'язаних зі збором даних та управлінням ними, які є частиною впровадження нової програми або технології. ОВК також важлива, коли контекст програми суттєво змінюється, і необхідно врахувати нові ризики або сценарії.

ОВК необхідна щоразу, коли нова програма, проєкт або технологія передбачає збір або використання персональних або чутливих даних.

☆ Важливість

ОВК дозволяє проаналізувати, як певний проєкт або нова технологія впливатиме на конфіденційність залучених осіб. ОВК також допомагає задокументувати стратегії зниження ризику, які захищають конфіденційність учасника та зміцнюють довіру громадськості до нашої роботи. ОВК гарантує, що потенційні проблеми будуть виявлені на ранній стадії, коли їх вирішення буде простішим, менш витратним і коли не буде ризику завдати шкоди учасникам програми або співробітникам.

Принципи

Принципи, що лежать в основі ОВК, аналогічні тим, що застосовуються для будь-якого безпечного використання персональних даних. Нижче наведено деякі ключові принципи, які було адаптовано з тих, що використовує Cash Learning Partnership (CaLP).

- Визначити ризики конфіденційності для окремих осіб.
- Визначити зобов'язання щодо дотримання вимог конфіденційності та захисту даних для своєї організації.
- Продемонструвати підзвітність та дотримання політик, які захищають учасників програми, партнерів і співробітників.
- Забезпечити, щоб організація просувала право на конфіденційність у своїй гуманітарній діяльності та виконувала функції етичного розпорядника даних.

Довідник

Співробітники Mercy Corps можуть знайти посібник із ОВК у цифровій бібліотеці. Документ містить відповіді на поширені запитання, пов'язані з ОВК, та посилання на внутрішній архів Mercy Corps виконаних ОВК для порівняння. Посібник із ОВК від Mercy Corps доступний усім англійською, арабською, іспанською, французькою та російською мовами.

Пам'ятайте:

- ОВК — це процес, який використовується для виявлення та мінімізації ризиків конфіденційності. Заповнення форми ОВК — це ще не кінець процесу! Поверніться до ОВК знову після того, як ваш проєкт почне працювати, аби переконатися, що не з'явилися нові зміни, які створюють нові ризики. Якщо такі є, задокументуйте зміни та нові стратегії пом'якшення наслідків, необхідні для мінімізації будь-яких нових ризиків.

- Проведення ОВК передбачає роботу з людьми в Mercy Corps, а іноді й з партнерськими організаціями та іншими для виявлення та зниження ризиків конфіденційності. Наприклад, якщо ви використовуєте нову технологію, вам, можливо, буде потрібно дослідити, чи має компанія, з якою ви працюєте, політику конфіденційності та які технологічні гарантії вони використовують для забезпечення захисту даних. Вам також може знадобитися ознайомитися з відповідними нормативними актами щодо конфіденційності у країні, де ви працюєте. Три вебсайти, які можна використовувати для моніторингу законів про дані та конфіденційність національного рівня:
  - Закони про захист даних у світі;
  - База даних законодавства про захист і конфіденційність даних у всьому світі Конференції ООН з торгівлі та розвитку;
  - База даних світових законів про конфіденційність OneTrust DataGuidance.
- Може бути корисно порівняти ОВК аналогічних програм. Ви можете провести це дослідження самостійно або звернутися по допомогу до команди захисту і конфіденційності даних.

Шаблони

Співробітники Mercy Corps можуть знайти детальний шаблон ОВК у цифровій бібліотеці. Детальний шаблон ОВК доступний усім англійською, арабською, іспанською, французькою і російською мовами.

Кожен детальний шаблон ОВК містить п'ять прикладів використання, які пояснено нижче. Натисніть на посилання нижче, і ви перейдете на сторінку, де будь-хто може завантажити англійські версії окремих прикладів використання у форматі **.odt** (сумісний із Microsoft Word та програмами з відкритим вихідним кодом, зокрема OpenOffice і LibreOffice), натиснувши кнопку **"Переглянути вихідні дані"** або **"Завантажити"**.

- нова Політика
- новий Процес або Процедура
- нове Програмне забезпечення або Технологічна система
  - Насамперед це стосується впровадження нових систем на глобальному рівні, у масштабах країни чи конкретної команди.
  - Якщо ви обираєте або використовуєте нову систему як частину більшого проєкту чи програми, використовуйте натомість опцію проєкту чи програми.
- новий Постачальник або Партнер
  - Насамперед це призначено для оцінки діяльності постачальника, партнера чи третьої сторони в рамках унікального або одноразового заходу.
  - Якщо ви обираєте або використовуєте нового постачальника, партнера чи третю сторону як частину більшого проєкту чи програми, використовуйте натомість опцію проєкту чи програми.
- новий Проєкт або Програма
  - Це може стосуватися будь-якого етапу чи аспекту проєкту чи програми.
  - Це найповніший варіант ОВК, і він включає мову для вибору нового програмного забезпечення або технологічних систем та/або нового постачальника чи партнера.

Додаткова підтримка

- "Початковий набір даних" від Electronic Cash Transfer Learning Action Network містить низку порад для ОВК **(див. листок порад №1)**.
- Офіс комісара з інформації Великобританії надає детальний кодекс правил для проведення оцінки впливу на конфіденційність.
- "Довідник із захисту даних у гуманітарній діяльності" від Міжнародного Комітету Червоного Хреста є докладним посібником майже з усіх аспектів гуманітарних даних. Глава 5 присвячена конкретно оцінці впливу на конфіденційність.

Найкращі практики спільного використання файлів

Цей посібник охоплює найкращі практики спільного використання файлів для членів команди Mercy Corps з використанням додатків G Suite, зокрема Google Мій диск. Щоб спростити цей посібник, ми обговорюватимемо спільний доступ до одного *файлу*, наприклад електронної таблиці. Однак, при спільному використанні *папки* Мій диск доступні такі самі можливості.

Примітка. Для організації спільного доступу до файлів Mercy Corps переходить на Microsoft 365. Після встановлення найкращих практик для цієї платформи буде створено аналогічний документ або ресурс.

☆ Важливість

Є кілька причин, чому краще поділитися файлом, розмістивши його на Google Диску та надіславши посилання замість вкладення в електронному листі.

- Безпека: ви можете легко змінити того, кому дозволено мати доступ або редагувати ваш файл. Ви також можете зробити посилання тимчасовим, надаючи доступ до файлу лише протягом певного проміжку часу.
- Керування версіями: під час спільного використання файлу, розміщеного онлайн, багато людей можуть одночасно отримати до нього доступ, і всі зміни та коментарі залишаться в одному файлі. Надсилання файлу як вкладення часто призводить до існування кількох версій одного документа з різними іменами файлів, редагуваннями, коментарями тощо. Власник документа витратить багато часу, намагаючись зібрати все це в один файл! Використання посилання також гарантує, що одержувачі завжди мають доступ до найновішої версії документа.
- Розмір файлів. Деякі IT-відділи накладають обмеження на дозволений розмір вкладень. Відправлення посилання дозволяє обмінюватися файлами будь-якого розміру.
- Легке редагування. Надання спільного доступу до файлів у форматі Google документи на Диску, Microsoft Word у OneDrive або подібних, дозволяє одержувачу відкривати документ і взаємодіяти з ним за допомогою веб-браузера: не обов'язково мати найновішу версію певного типу програмного забезпечення.

Принципи

Щоразу, коли надаєте спільний доступ до документів, ви повинні враховувати таке.

- **Добре подумайте, хто створить файл або папку, хто буде володіти ними/адмініструвати їх і хто матиме до них доступ. Якщо тимчасові підрядники створюють і адмініструють файли, існує ризик того, що файли або доступ залишаться у них після завершення співпраці!**
  - Надавайте доступ лише тим, кому файл потрібен.
  - Вміст конфіденційної, особистої інформації або інформації, що ідентифікує особу (ІІО), завжди повинен мати обмежений доступ. Якщо ви не можете визначити, чи слід обмежувати доступ до вмісту або як це зробити, будь ласка, зверніться по допомогу до юридичної команди або команди із захисту даних та конфіденційності.

❭ Використовуйте відповідний рівень дозволів.

- Розглянемо приклад, коли потрібно створити новий статут проєкту. Швидше за все, повний доступ повинна мати лише команда, відповідальна за створення статуту. Коли прийшов час отримувати зворотний зв'язок від інших, надайте додаткові дозволи, які дозволяють лише переглядати або коментувати.
- Будьте вкрай обережні, надаючи запити на доступ членам команди, які можуть випадково користуватися своїми особистими обліковими записами електронної пошти. Замість того, щоб надавати доступ через особистий обліковий запис електронної пошти, надайте доступ через обліковий запис Mercy Corps і попросіть члена команди увійти за допомогою цих облікових даних.

❭ Дозволи змінюються з часом

- Якщо ви працюєте з кимось лише тимчасово або з людьми за межами Mercy Corps, розгляньте надання тимчасових дозволів. Встановіть дату припинення доступу. Це забезпечить своєчасне обмеження доступу, у разі якщо ви забудете це зробити пізніше.
- Періодично перевіряйте список тих, хто має доступ до ваших файлів, папок або спільних дисків, щоби забезпечити видалення доступу тих членів команди, у яких змінилася роль або які більше не працюють із Mercy Corps.

❭ Небезпечний вміст вимагає додаткових кроків

- Інформація, що ідентифікує особу (ІІО), інформація, що ідентифікує демографічну належність (ІДН), або інші типи персональних даних захищені численними законами про захист даних. Перш ніж передавати персональні дані, перевірте юридичні вимоги щодо передачі цієї інформації іншим. Неналежна передача персональних даних може поставити під загрозу учасників програми, донорів, партнерів і членів команди Mercy Corps. Якщо у вас є питання щодо законів про персональні дані або захист даних, будь ласка, напишіть команді із захисту та конфіденційності даних на адресу dataprotection@mercycorps.org.
- Якщо інформація вважається конфіденційною або службовою для ділових цілей, діліться нею лише з тими сторонами, з якими необхідно, та подумайте про надання тимчасового доступу.
- Якщо особа, яка отримує файл, працює в небезпечному місці, або якщо вміст файлу містить персональні дані, подумайте про шифрування файлу або захист його паролем. Приклади того, як це зробити, дивіться в розділах "Шифрування" та "Знеособлення".

❭ Ніколи не переміщуйте файли без дозволу власника.

- Переміщення файлів може змінити коло осіб, які мають доступ, і зробити пошук файлу неможливим для інших! Завжди уточнюйте у власника документа, перш ніж переміщувати спільний файл у нове місце.

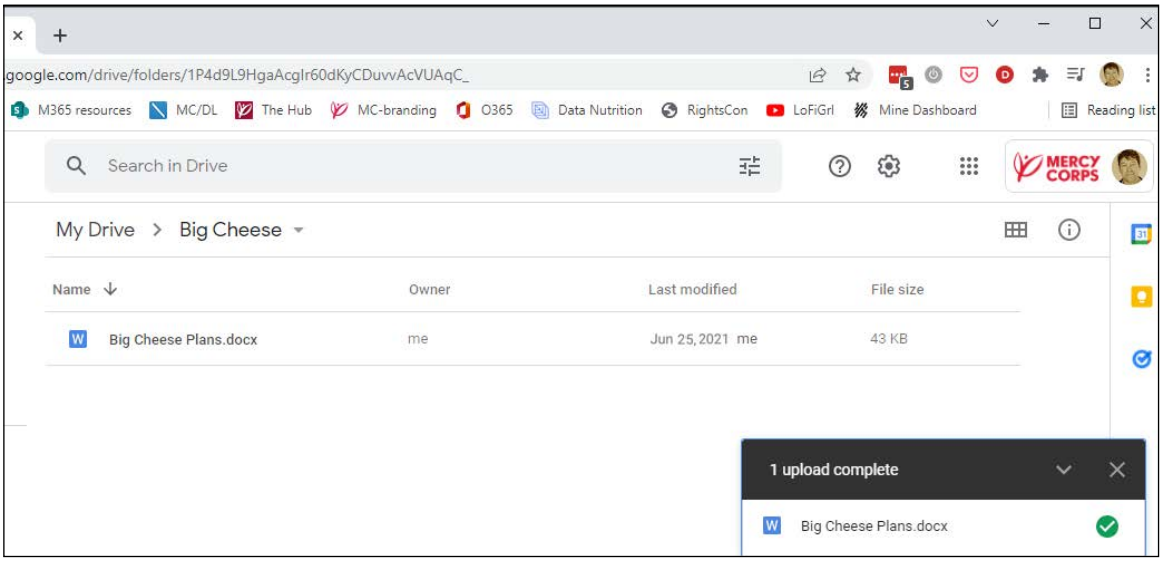
Спільний доступ до файлів GDrive

Ось приклад використання спільного доступу до файлу на Google Диску із застосуванням найкращих практик. Уявіть, що зараз 2020 рік і Mercy Corps працює з консультантом (PNW Rocks), щоби створити матеріали для великої нової ініціативи в Mercy Corps із кодовою назвою "Шишка". Про проєкт "Шишка" не буде оголошено публічно до липня 2021 року, тому важливо обмежити коло осіб, які мають доступ до файлу. Для початку ми хочемо разом працювати над наступними кроками для проєкту у файлі під назвою "Плани шишки".

Інструкції

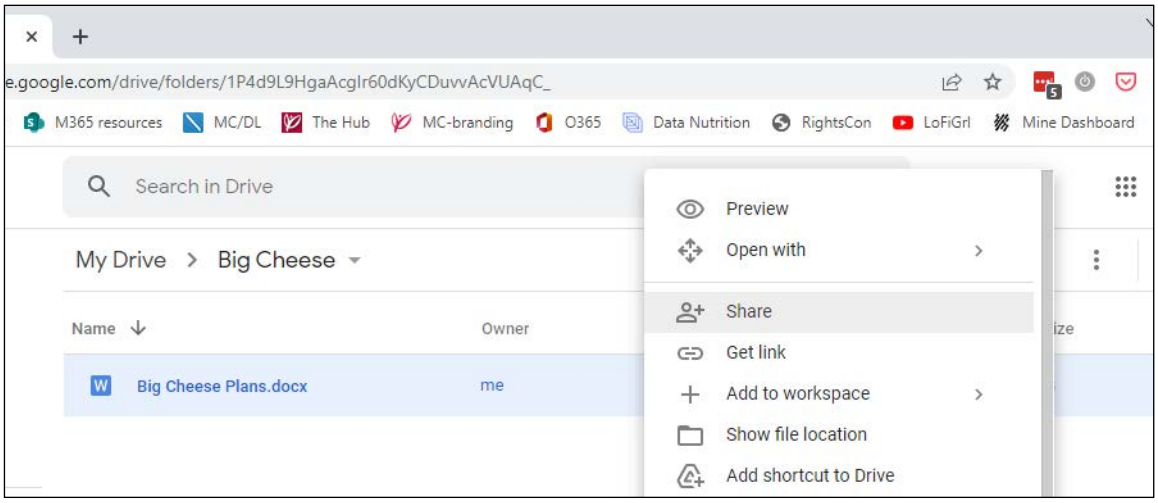
Крок 1 — завантажити

Завантажте файл на Мій диск.



Крок 2 — поділитися

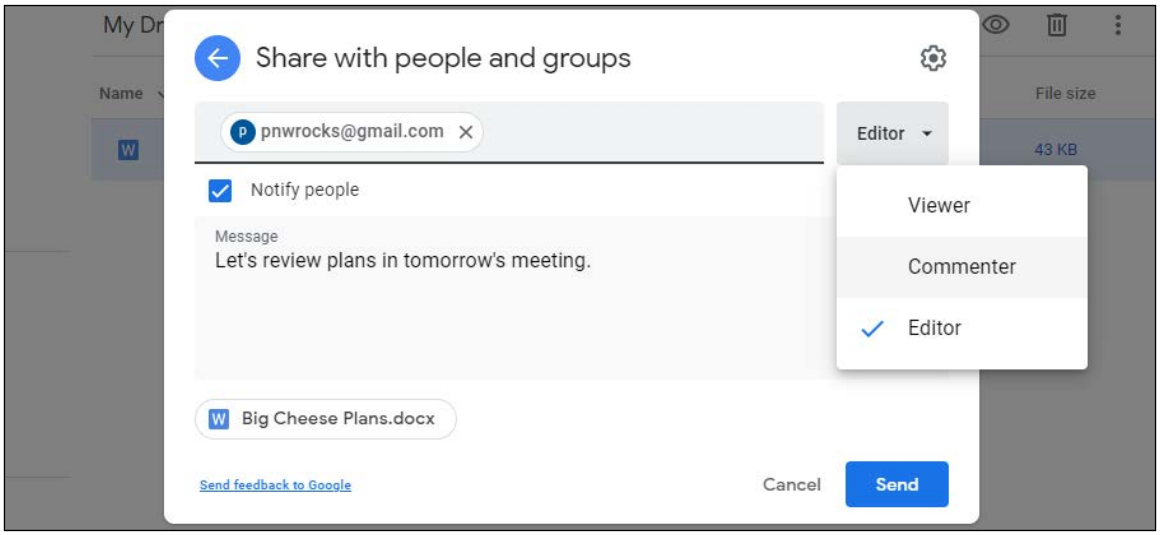
Щоби надати спільний доступ до файлу, клацніть по ньому правою кнопкою миші та виберіть команду **"Поділитися"**.



- Надавайте доступ лише тим, кому файл потрібен. Коли ви надаєте спільний доступ до файлу на Моєму диску, за замовчуванням встановлюється **"Обмежений доступ"** (для осіб і груп), що є найбільш ефективним варіантом. Пам'ятайте, вміст конфіденційної, особистої інформації або інформації, що ідентифікує особу (ІІО) завжди повинен мати обмежений доступ!
- Параметр **"Усі, хто має посилання"** повинен використовуватися лише для файлів, які не містять конфіденційної інформації та відкриті для громадськості. Якщо параметр **"Усі, хто має посилання"**використовується для файлу з конфіденційними особистими, персональними або фінансовими даними, такий файл може легко і випадково стати публічним, поставити Mercy Corps під загрозу безпосереднього юридичного ризику і полегшити небезпечним людям використання інформації в злочинних цілях.

Крок 3 — обрати рівень доступу

Введіть адресу електронної пошти людини, якій ви хочете надати спільний доступ, а потім виберіть рівень доступу. Google за замовчуванням надає доступ **"Редактор"**, який підходить лише для членів команди, яким потрібен повний доступ до документа. Коли ви залучаєте зацікавлені сторони для зворотного зв'язку, оберіть доступ **"Читач"** або **"Коментатор"**. Найкраща практика — сповістити особу та додати повідомлення, в якому пояснюється, чому ви надали спільний доступ до цього файлу. Щоби сповістити, поставте відмітку біля **"Сповістити"**. Завершивши зміни, натисніть **"Надіслати"**.

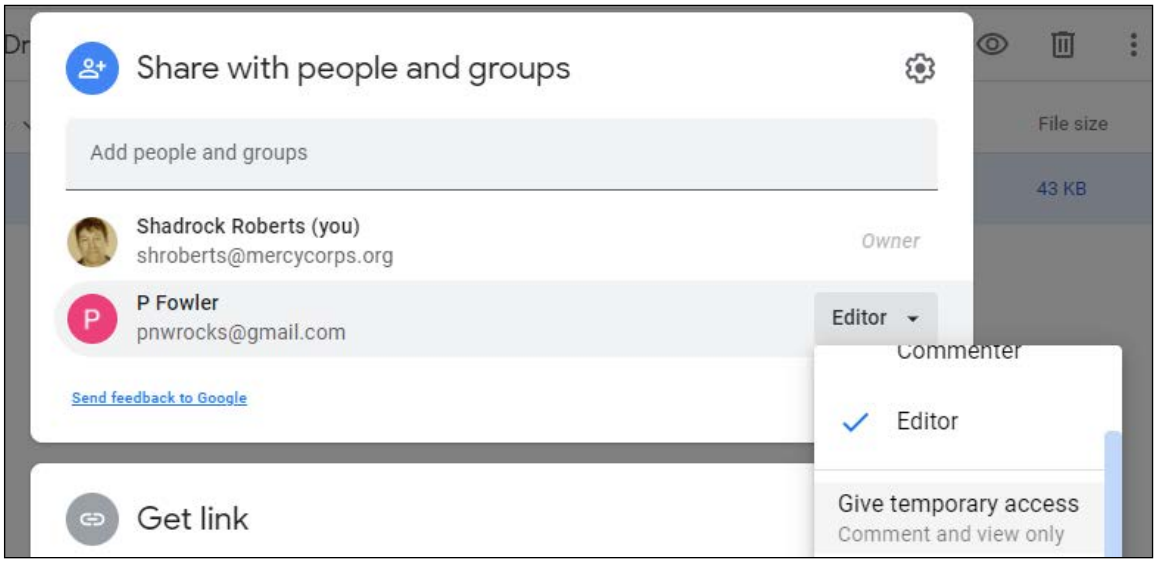


Інший варіант — відправити окремий електронний лист із посиланням на файл. Щоби повідомити окремо електронною поштою, зніміть відмітку біля **"Сповістити"**. Після натискання **"Готово"**клацніть по файлу правою кнопкою миші та оберіть **"Отримати посилання"**. У новому спливаючому вікні натисніть кнопку **"Копіювати посилання"**, а потім вставте його у свій електронний лист.

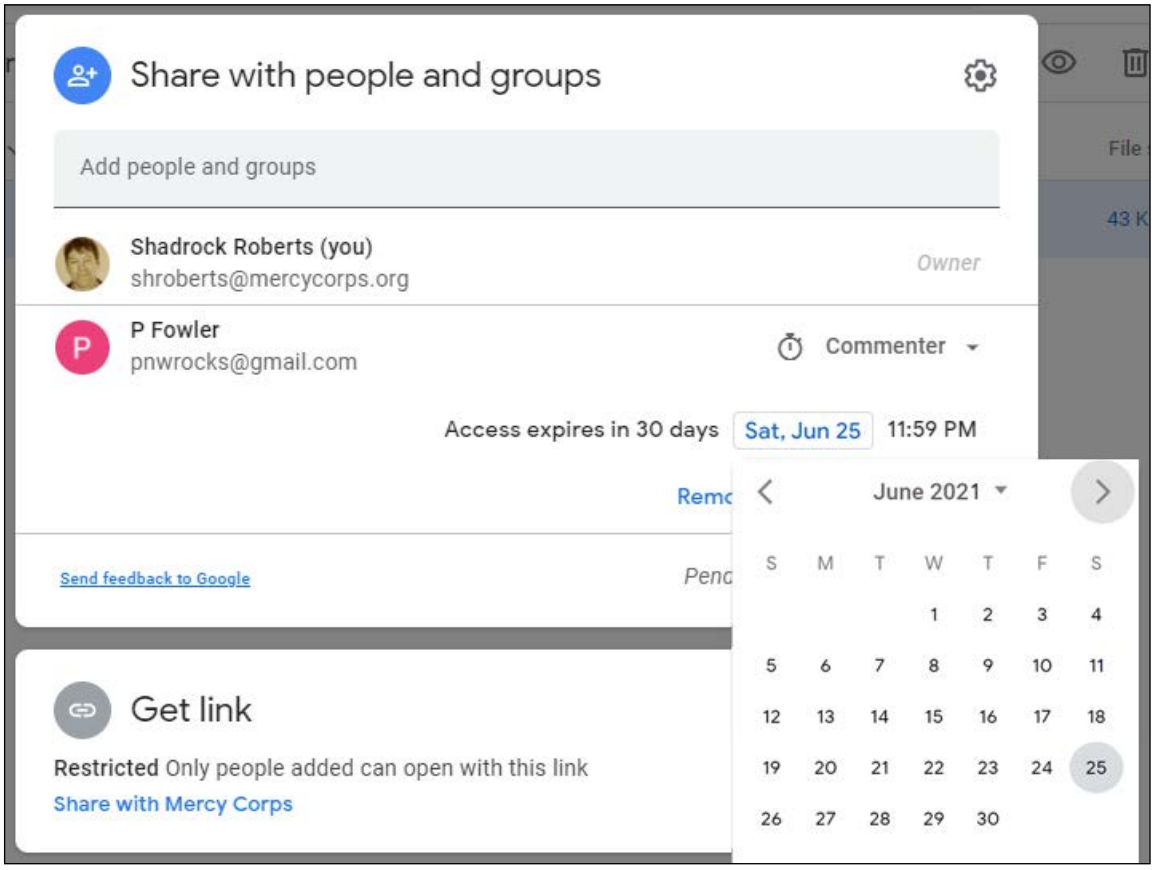
- Щоби дізнатися більше про рівні доступу, зайдіть у розділ "Спільний доступ і співпраця на Моєму диску".
- Якщо ви обмежите доступ до файлу, а хтось із доступом поділиться посиланням з іншою особою, ця особа не матиме автоматично доступу до цієї інформації на Google Диску. Замість цього вона побачить веб-сторінку, де можна запросити доступ. Запит на доступ надійде власнику файлу. Запити на доступ потрібно переглядати, а ті, хто отримує їх, не повинні надавати дозвіл на будь-які запити, не ознайомившись із вищенаведеними примітками та міркуваннями.

Крок 4 — тимчасовий доступ

Після надання дозволу термін спільного доступу можна скоротити. Щоб обмежити доступ, клацніть по файлу правою кнопкою миші ще раз і клацніть на **"Поділитися"**. Знайдіть адресу електронної пошти, за якою ви щойно надали спільний доступ, і клацніть правою кнопкою миші на рівень доступу. Ви побачите нові параметри; оберіть **"Надати тимчасовий доступ"**.



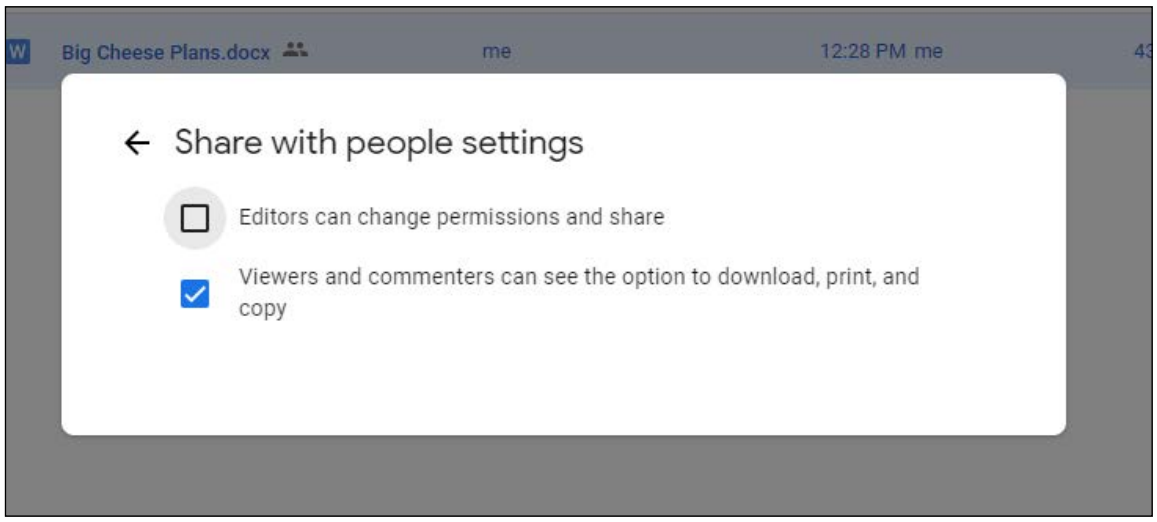
З'явиться календар. Перейдіть до місяця, коли термін дії доступу має закінчитися, і оберіть відповідну дату.



Календар зникне, а показана дата зміниться. Побачивши, що дата закінчення терміну доступу правильна, натисніть **"Зберегти"**.

Крок 5 — додаткові параметри

Якщо у вас є побоювання, що інші можуть вчинити неналежні дії із вмістом, на екрані налаштувань є додаткові параметри. Доступ до параметрів файлу можна отримати через піктограму шестерні у верхньому правому куті вікна спільного доступу. Натисніть на шестерню, і ви побачите варіанти обмеження подальшого спільного використання або вимкнення можливості завантаження, друку або копіювання. Для будь-якої функції, яку ви хочете вимкнути, просто зніміть відмітку. Файл швидко оновиться, зберігши нове налаштування.



❱ Щоби дізнатися більше, зайдіть у розділ "Можливості обмеження спільного доступу на Диску".

Додаткові міркування

- Не розміщуйте конфіденційні файли у папках, які знаходяться у спільному доступі в багатьох людей. Дозволи спільних папок поширюються на кожен файл і вкладену папку, тому доступ до вашого конфіденційного файлу може отримати будь-хто, хто має дозвіл на доступ до головної папки! Замість цього перемістіть конфіденційний файл до нового місця за межами більшої структури спільних папок.
- Після надання спільного доступу до файлу у вас може бути можливість **"Зробити копію"** та/або **"Перемістити"** файл в інше місце. Ніколи не переміщуйте файл без дозволу власника!
- Якщо вам потрібно переглянути файл на Моєму диску або в іншому місці, найкраще буде використати параметр "Додати ярлик на Диск".
- Якщо зроблено копію файлу або файл переміщено, майте на увазі, що він не матиме тих самих дозволів, що й вихідний файл, якщо ви спеціально не встановите ці дозволи.

У цьому посібнику не розглядається спільний доступ до файлів на спільних дисках Google, а також зовнішні платформи спільного доступу до файлів. Щоби більше дізнатися про це, зайдіть на сторінку Google "Найкращі практики для спільних дисків" або "Керування спільними дисками". Кожна з цих сторінок доступна різними мовами: прокрутіть униз сторінки, щоби вибрати свою мову.

Найкращий спосіб контролювати доступ до файлів за допомогою Диска — це створити групу Google і надати дозволи тим, хто входить до неї. Групи Google призначені не лише для надсилання електронних листів; групи є потужним і зручним інструментом для керування дозволами доступу до папок і файлів. Дізнайтеся більше про Групи Google.

Якщо ваш проєкт вимагає використання додатків поза межами G Suite, запропонуйте своїй команді завантажити Google Диск для робочого стола. Ця програма дозволяє переглядати будь-які документи на Моєму диску або Спільних дисках так, ніби вони знаходяться на вашому ноутбуці, навіть в автономному режимі й без необхідності завантажувати документ або конвертувати його у формат Google.

Додаткова підтримка

Те, як і з ким ви будете ділитися даними, має бути частиною ширшої стратегії життєвого циклу даних програми або заходу. Є кілька ресурсів, які можуть вам допомогти.

- "Збірник даних" від Міжнародної Федерації Товариств Червоного Хреста і Червоного Півмісяця (IFRC) є відмінним ресурсом вправ, планів занять, контрольних списків та інших матеріалів, які допоможуть вам організувати бесіди та заходи зі своєю командою. Зокрема, варто почати з Модуля 7 — обмін даними.
- "Довідник із захисту даних у гуманітарній діяльності" від Міжнародного Комітету Червоного Хреста є докладним посібником майже з усіх аспектів гуманітарних даних. Глава 2 спеціально присвячена обміну даними.
- "Інструментарій відповідальності за дані" від Cash Learning Partnership призначений спеціально для тих, хто використовує готівку та ваучери, але є "золотим стандартом" настанов із відповідального ставлення до даних. Дивіться зокрема лист порад №6, "Обмін даними". Інструментарій доступний англійською, арабською, французькою й іспанською мовами.

Знеособлення даних

У цьому посібнику наведено приклад видалення з набору даних інформації, що ідентифікує особу (ІІО). Існує кілька способів «знеособлення» даних, під якими розуміють заходи або методи обробки, спрямовані на запобігання розкриттю особистості суб'єкта даних. Два поширених типи знеособлення — "анонімізація" і "псевдонімізація".

Анонімізація — це процес, за допомогою якого персональні дані стають анонімними, щоб особу (або "суб'єкт даних") більше не можна було ідентифікувати. Це постійна зміна даних. Загальні методи включають в себе видалення інформації, що ідентифікує особу, або шифрування значень у певних наборах ІІО.

> Приклад: уявіть, що організація має дані опитування, які містять поля для імені, державного ідентифікаційного коду, назви села, етнічної належності, віку, рівня освіти та показників здоров'я. У цьому випадку видалення імені та державного ідентифікаційного коду буде першим кроком до того, щоби зробити дані анонімними, оскільки ці «прямі характеристики» є персональними даними, які безпосередньо ідентифікують особу. «Непрямі характеристики» — назва села, етнічна належність, вік, рівень освіти та показники здоров'я залишаться.

Однак, попри те, що деякі характеристики здаються "анонімними", вони можуть такими не бути. Якщо опитування проводилося в дуже маленькому селі, де лише двоє жителів ідентифікують себе із певною етнічною належністю, і вони різного віку, то використання цих двох непрямих характеристик може дозволити ідентифікувати цих людей! Процес, у ході якого досліджуються всі атрибути для зниження ризику повторної ідентифікації суб'єкта даних, називається статистичним контролем розкриття даних. Першим кроком у цьому процесі є оцінка ризиків розкриття даних. У Центрі гуманітарних даних є навчальний онлайн-посібник для проведення оцінки ризику розкриття даних.

Псевдонімізація, з іншого боку, полягає в обробці персональних даних таким чином, що персональні дані більше не може бути віднесено до конкретного суб'єкта даних без використання додаткової інформації, такої як ключовий код.

> Приклад: уявіть, що опитування містить ваше ім'я, адресу електронної пошти, вік, національність і робоче місце. Псевдонімізація бере дані, за якими можна ідентифікувати конкретно вас (ваше ім'я, адресу електронної пошти, вік), і робить їх недоступними та відокремленими від неспецифічних даних, таких як ваша національність. Псевдонімні дані може бути знову зібрано разом в якийсь момент, так що всю інформацію може бути знову пов'язано з конкретним джерелом або особою. Ось чому псевдонімізація вимагає, щоби додаткова інформація зберігалася окремо і підлягала технічним та організаційним заходам для забезпечення неможливості віднесення персональних даних до суб'єкта даних.

Що обрати — анонімізацію або псевдонімізацію?

Анонімізація, як правило, буде безпечнішою та зменшить ризик розкриття ІІО. Однак іноді це може зробити дані занадто загальними, через що вони можуть втратити користь для таких програм, як робота з грошовими ваучерами. У випадку програм охорони здоров'я, які включають вакцинацію або інші методи лікування, може бути важливо зв'язатися з людьми для подальшого лікування. В обох цих випадках псевдонімізація буде найкращим вибором, оскільки ви завжди можете знову зібрати дані разом, щоби ідентифікувати особу, коли це необхідно.

Немає єдиної правильної відповіді на те, коли віддавати перевагу одному методу перед іншим, і перш ніж обрати, як знеособити свої дані, важливо розуміти, чому дані було зібрано, потенційні ризики, пов'язані зі зберіганням цих даних, і потреби програми.

Важливо також розуміти, що методи, які використовуються як для анонімізації, так і для злому даних, стають все складнішими, і що навіть знеособлені дані не завжди на сто відсотків в безпеці. Якщо сумніваєтеся, зверніться по допомогу до своєї команди з даних або IT.

☆ Важливість

Останні витоки даних у Міжнародному Комітеті Червоного Хреста, зломи електронної пошти в Агентстві США з міжнародного розвитку та неналежне розповсюдження даних Верховним Комісаром ООН у справах біженців — все це показує, яким чином гуманітарні дані наражаються на ризик. Дані опитувань домогосподарств, оцінки потреб та інші форми мікроданих складають все більш значний обсяг даних у гуманітарному секторі. Ці типи даних мають вирішальне значення для визначення потреб і перспектив учасників програми та спільнот, у яких ми працюємо, але ці дані також пов’язані з певними ризиками. Розуміння того, як оцінювати та керувати чутливістю цих даних, має дуже важливе значення для забезпечення їх безпечного, етичного та ефективного використання в різних контекстах реагування.

Деякі переваги використання анонімізованих даних над персональними даними:

- - захист від неналежного розкриття персональних даних;
- - до анонімізованих даних застосовується менше юридичних обмежень;
- - надання організаціям можливості створювати відкриті або загальнодоступні дані, дотримуючись при цьому своїх зобов'язань щодо захисту даних.

Принципи

Знеособлення даних є частиною обробки даних, а обробка персональних даних, здійснювана гуманітарними організаціями, повинна відповідати наступним принципам.

- **Справедливість і законність обробки:** методи повинні відповідати регіональному, національному чи місцевому законодавству або політиці, які можуть обмежувати те, які дані може бути знеособлено і як використовуються певні технології. Будь-яка обробка персональних даних має бути прозорою для залучених суб'єктів даних.
- **Обмеження цілей:** гуманітарні організації повинні визначити та викласти конкретні цілі, для яких обробляються дані. Ці цілі повинні бути чіткими та законними.
- **Пропорційність:** забезпечити, щоби кожен конкретний захід, пов'язаний з обробкою персональних даних, відповідав заявленій меті. Наприклад, чи збирається лише мінімально необхідний обсяг даних? Чи вжито відповідні технічні та організаційні заходи для зменшення ризиків, пов'язаних з обробкою даних?
- **Технологічні зміни:** нові набори даних та нові інструменти для їх аналізу швидко змінюються та розвиваються, як і засоби, за допомогою яких дані зламують або крадуть. Важливо розуміти нові та потенційні ризики для ваших даних і продовжувати коригувати свої методи та практики відповідним чином.

Псевдонімізація

Це приклад одного зі способів знеособлення даних в електронній таблиці. Існує широкий спектр способів знеособлення. У цьому прикладі використовується «ключовий код» для видалення інформації, що ідентифікує особу, знайденої в прямих ідентифікаторах, і збереження її в окремому файлі. Інформація, що ідентифікує особу, (ІІО) — це інформація, яка може бути використана для визначення особи. Типовими прикладами є повне ім'я, адреса, номер телефону, дата народження та номер соціального забезпечення або національний ідентифікаційний код.

Інструкції

Ви можете слідувати цим Інструкціям із псевдонімізації, щоби розглянути базовий приклад псевдонімізації набору даних. У цій вправі використовується зразок набору даних, знайдений у папці з даними онлайн-посібника.

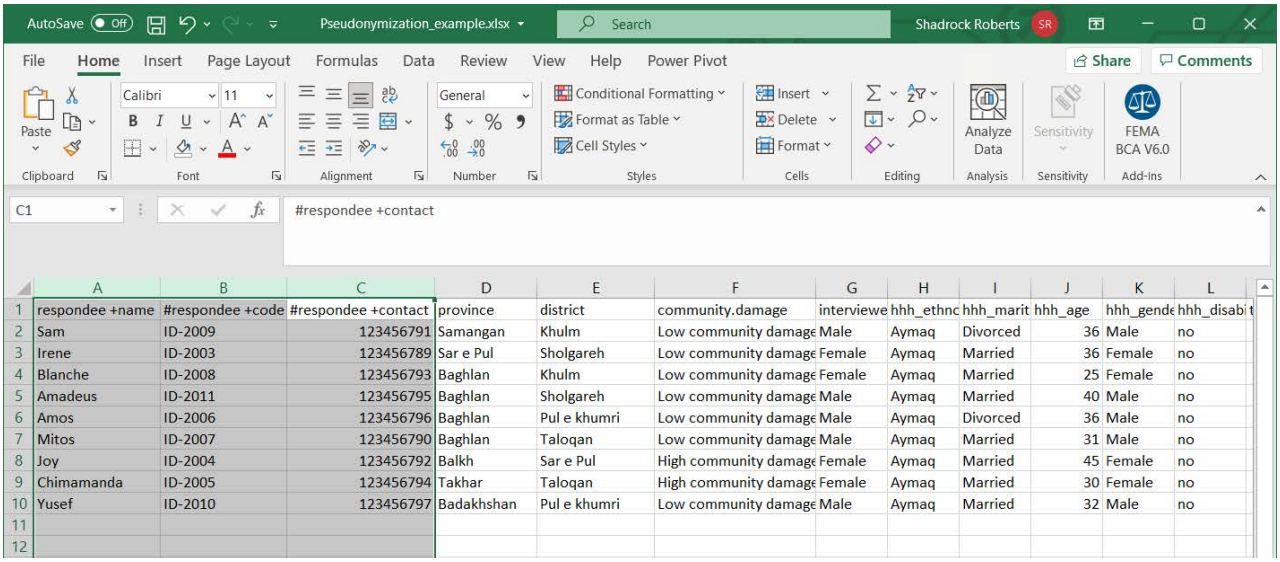
Після псевдонімізації зразка даних ви можете продовжити роботу з навчальним посібником від Центру гуманітарних даних для проведення оцінки ризиків розкриття даних.

Крок 1 — визначте ІІО

Почніть із виявлення ІІО в даних. В ідеалі у вас будуть метадані — дані або документ, який визначає ваші дані, — щоби допомогти вам зрозуміти, які поля містять ІІО. У зразку даних є три стовпці, які містять потенційну ІІО:

- **№ респондента +ім'я**, схоже, містить ім'я.
- **№ респондента +код**, ймовірно, містить якийсь ідентифікаційний номер.
- **№ респондента +контакт**, можливо, містить номер мобільного телефону

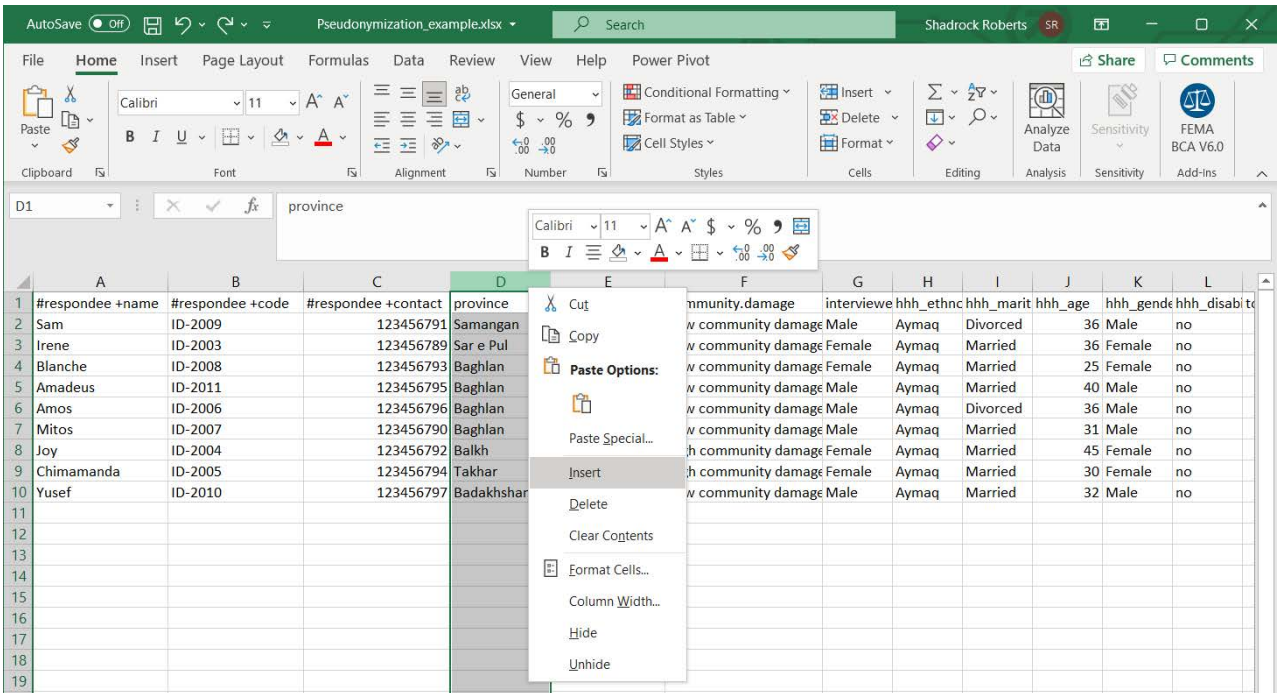
Кожен із цих прямих ідентифікаторів використовує гуманітарну мову обміну для позначення даних.



	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 t
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												

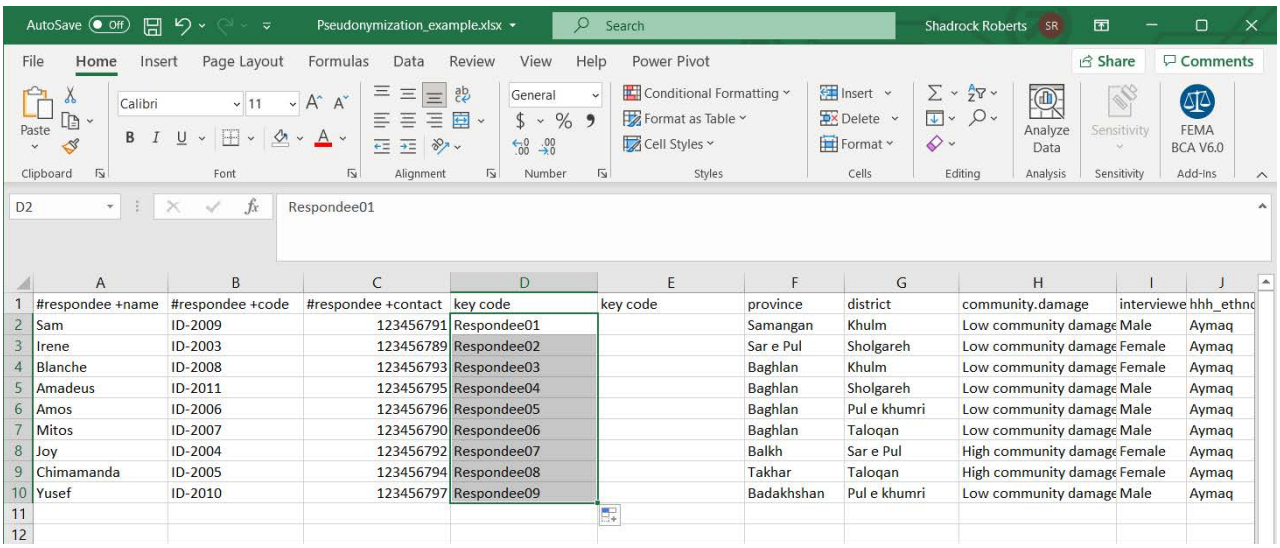
Крок 2 — створіть нові стовпці для ключового коду

Ми будемо використовувати ключовий код, значення, яке ми генеруємо, щоби розбити ІІО. Оскільки всі прямі ідентифікатори згруповані разом, ми створимо два нових стовпці між стовпцем C, **№ респондента +контакт** і стовпцем D, **область**. У Excel ми робимо це, виділяючи стовпець праворуч від того місця, куди ми хочемо вставити нові стовпці. Клацніть правою кнопкою миші на стовпці та оберіть **"Вставити"**. Повторіть цей процес ще раз, щоби створити ще один пустий стовпець.



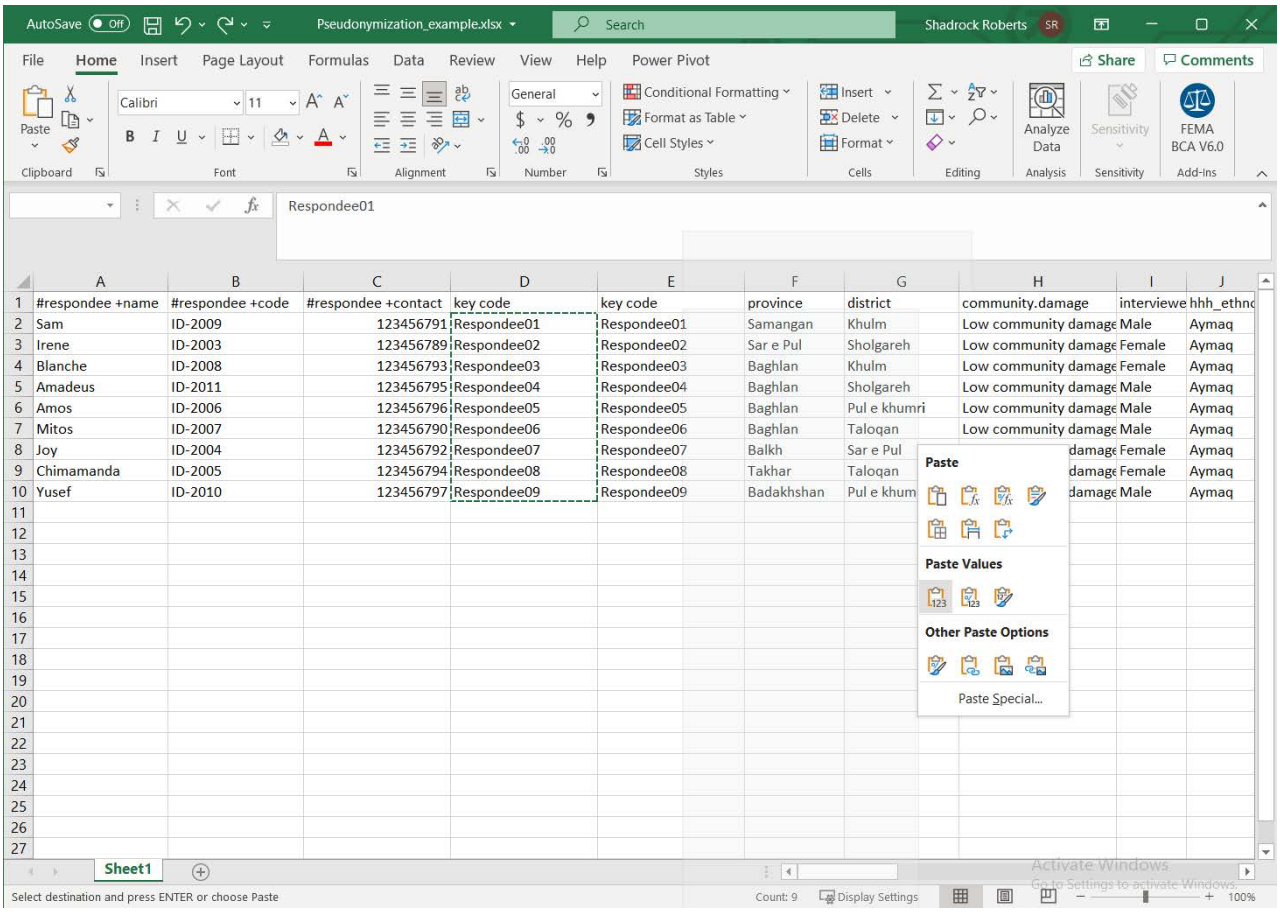
Крок 3 — створіть ключовий код

Почніть з іменування нових стовпців. Ми будемо використовувати "ключовий код" у кожному з них: кожен стовпець буде містити однакові значення. Зараз саме час оновити всі метадані цього набору даних, щоби пояснити, що означає **ключовий код** ! Далі ми скористаємося функцією Excel "Автозаповнення" для створення простого коду. Введіть **Респондент01** у першу комірку. Далі виділіть цю комірку, натисніть на маркер перетягування в правому нижньому кутку комірки та перетягніть його вниз до кінця набору даних. Це автоматично заповнить остаточний номер кожного запису, щоб кожен респондент тепер мав новий код.



Крок 4 — дублювання ключового коду та видалення формул

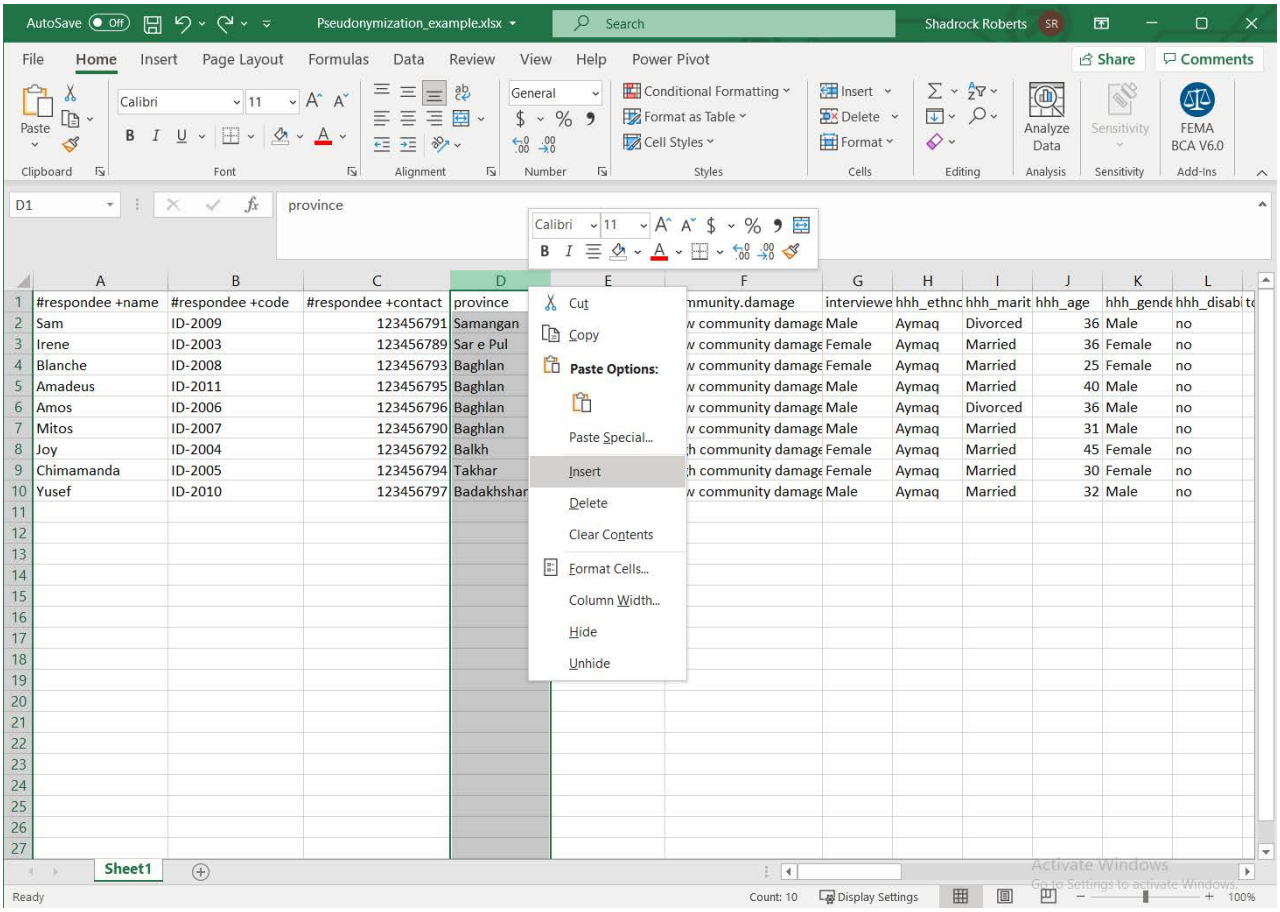
Тепер скопіюємо ключовий код і вставимо його в сусідній стовпець. Зробити це можна за допомогою основних клавіатурних команд, зокрема **ctrl + C**, або виділіть комірки, які потрібно скопіювати, клацніть на них правою кнопкою миші та оберіть **"Копіювати"**. У сусідньому стовпці виділіть комірки, в які потрібно вставити новий ключовий код, клацніть правою кнопкою миші та оберіть **"Вставити"**. Ми вирішили спеціально вставити лише значення. Якщо для створення нового коду ви використовували формулу, то важливо буде зберегти лише значення для використання як коду ключа!



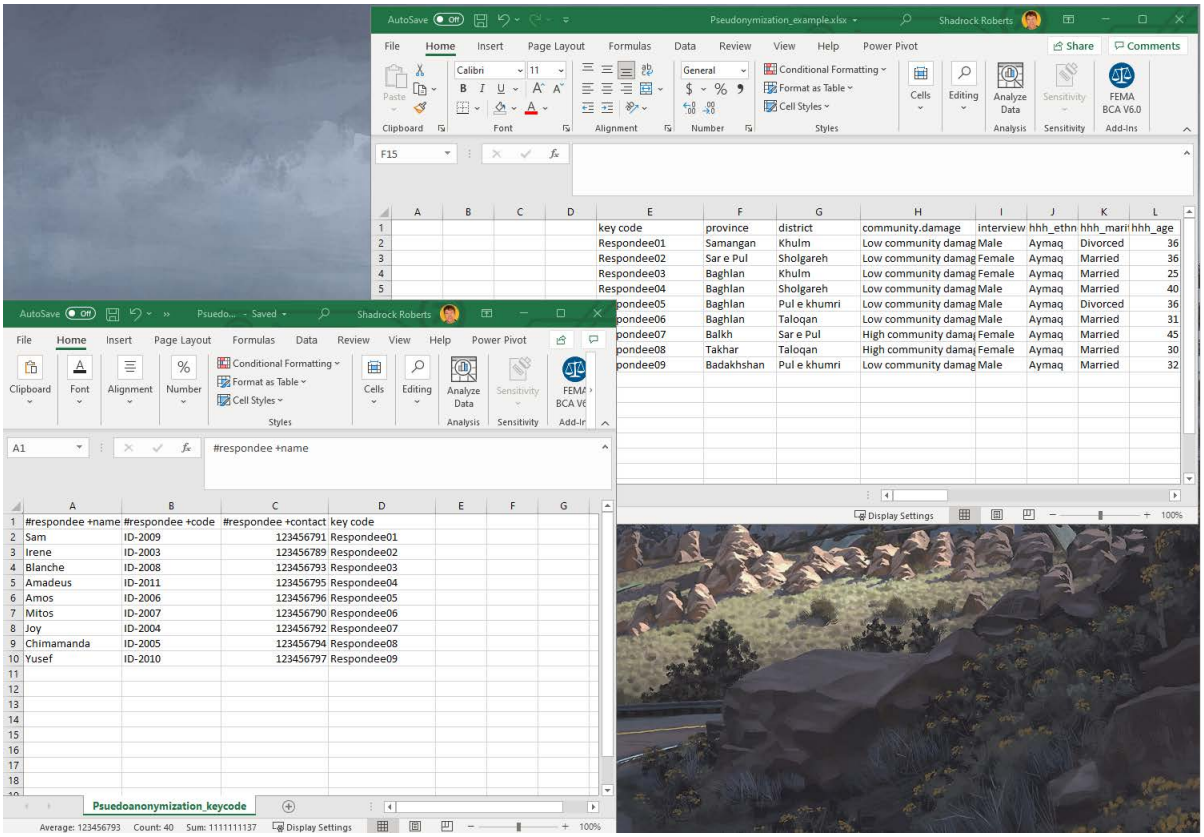
	A	B	C	D	E	F	G	H	I	J
1	#respondee +name	#respondee +code	#respondee +contact	key code	key code	province	district	community.damage	interviewe	hhh_ethn
2	Sam	ID-2009	123456791	Respondee01	Respondee01	Samangan	Khulm	Low community damage	Male	Aymaq
3	Irene	ID-2003	123456789	Respondee02	Respondee02	Sar e Pul	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

Крок 5 — відокремте прямі та непрямі ідентифікатори

Виділіть стовпці, які містять прямі ідентифікатори з ІІО, а також один із стовпців із ключовим кодом. У цьому прикладі ми виділяємо стовпці A-D. Клацніть на них правою кнопкою миші та оберіть **"Вирізати"**.



Далі відкрийте нову електронну таблицю та вставте ці значення за допомогою комбінації клавіш **ctrl + V** або іншим способом. Збережіть нову електронну таблицю. Тепер у вас є дві електронні таблиці: одна з них містить непрямі ідентифікатори, тоді як новий аркуш містить прямі ідентифікатори з ІІО. Обидва набори даних містять ключовий код для кожного запису в даних, щоб усі дані можна було об'єднати, коли це необхідно.



Наступні кроки

Обидва файли містять ключовий код, який дозволить знову об'єднати їх. Одним зі способів зробити це в Excel є використання функції VLOOKUP для автоматичного заповнення комірок на основі значення інших комірок. У цьому випадку можна заповнити пусті комірки у вихідному файлі відсутньою ІІО на основі значення **ключового коду**.

Оскільки новий файл містить прямі ідентифікатори з ІІО, його потрібно надійно зберігати. Один чудовий спосіб зробити це — зашифрувати файл і використовувати хмарне сховище, щоб обмежити кількість тих, хто має доступ до файлу (**дивіться посібники з найкращих практик шифрування та обміну файлами**).

Пам'ятайте: хоча оригінальна електронна таблиця була знеособлена шляхом видалення прямих ідентифікаторів, які містять очевидну ІІО, інші непрямі ідентифікатори можуть бути об'єднані з іншими даними або проаналізовані таким чином, що це дозволить ідентифікувати особу.

З цієї причини обидва файли слід надійно зберігати. Якщо ви хочете надати ширший доступ до оригінального файлу, без ІІО, вкрай важливо виконати *оцінку ризиків розкриття даних*, щоби забезпечити мінімальний ризик повторної ідентифікації даних. Центр гуманітарних даних має навчальний онлайн-посібник для проведення оцінки ризиків розкриття даних із використанням статистичного програмного забезпечення "R" із відкритим вихідним кодом. Крім того, веб-сторінка Poverty Action Lab "Знеособлення для публікації даних" містить чудове обговорення знеособлення даних і зразок коду для статистичного програмного забезпечення Stata. Співробітники Mercy Corps мають внутрішній доступ до Проєкта настанов від T4D, де є додаткові формули Excel.

Нарешті, всі ці кроки разом допомагають зменшити ризик розкриття ІІО, тому вони повинні бути перераховані в ОВК (**дивіться посібник з оцінки впливу на конфіденційність**), щоб інші розуміли, яким чином ці дані захищені.

Додаткова підтримка

Знеособлення даних є частиною практик належного керування даними та більшого життєвого циклу даних, що є загальною діяльністю для індивідуального збору даних як складової програми або відгуку. Наступні ресурси є відмінним початком для повнішого розуміння управління вашими даними відповідальним чином.

- "Інструментарій відповідальності за дані" від Cash Learning Partnership призначений спеціально для тих, хто використовує готівку та ваучери, але є золотим стандартом управління відповідальним використанням даних. Інструментарій доступний англійською, арабською, французькою й іспанською мовами.
- *"Набір для початківців про дані для працівників гуманітарної сфери"* від Electronic Cash Transfer Learning Action Network містить низку порад щодо даних для розуміння різних аспектів практик належного керування даними та їх захисту.
- *"Довідник із захисту даних у гуманітарній діяльності"* від Міжнародного Комітету Червоного Хреста є докладним посібником майже з усіх аспектів гуманітарних даних. Глава 2 спеціально присвячена знеособленню даних.
- *"Довідник спеціаліста із сучасного розвитку"* від Engine Room — хороший огляд питання даних у контексті міжнародної діяльності з розвитку. Розділ про *"Обмін даними"* спеціально присвячений знеособленню.

Шифрування файлу

У цьому розділі розглядається простий приклад шифрування файлу за допомогою функції Microsoft, доступної на комп'ютерах Mercy Corps. Є цілий ряд факторів, які слід враховувати при шифруванні файлу, але тут ми зосередимося на використанні пароля та шифруванні одного файлу. Дивіться нижче посилання на ресурси, які досліджують шифрування глибше. Щодо цього посібника, однак, корисно зрозуміти тонку різницю між "захистом паролем" та "шифруванням".

Уявіть захист паролем як коробку з замком на ній. Коли ви "захищаєте паролем" свій документ, ви кладете його в електронну коробку і закриваєте паролем — відкрити коробку можуть лише ті, хто має пароль. Однак, якщо обраний вами пароль не дуже надійний, або якщо ви поділилися ним не з тією людиною, хтось може легко потрапити в цю коробку і переглянути ваш документ! На відміну від цього, шифрування використовує складні алгоритми для кодування інформації, що вимагає наявності ключа для розшифровки цієї інформації. Уявіть це, ніби ви взяли документ і пропустили його через шредер, на якому є спеціальна кнопка, щоби знову зібрати документ в одне ціле.

Коли ви поєднуєте захист паролем і шифрування, то ефективно подвоюєте свій захист. Якщо хтось успішно зламає пароль до електронної коробки, він зможе побачити лише шматочки подрібненого паперу, якщо не має відповідного ключа. Усі ноутбуки Mercy Corps зашифровано за допомогою Microsoft BitLocker. Це запобігає тому, щоби жорсткий диск ноутбука Mercy Corps можна було вийняти та отримати до нього доступ на іншому комп'ютері.

☆ Важливість

Шифрування дуже важливе, оскільки воно допомагає забезпечити конфіденційність та безпеку інформації. Без шифрування дані можуть бути перехоплені та прочитані будь-якою людиною, яка має до них доступ. При розгляді питання про те, чи потрібно шифрувати дані, запитайте себе: "Який існує ризик для учасників програм, співробітників і партнерів Mercy Corps у разі втрати або крадіжки цих даних?" Хороше практичне правило — шифрувати все, що містить інформацію, що ідентифікує особу, або чутливу інформацію.

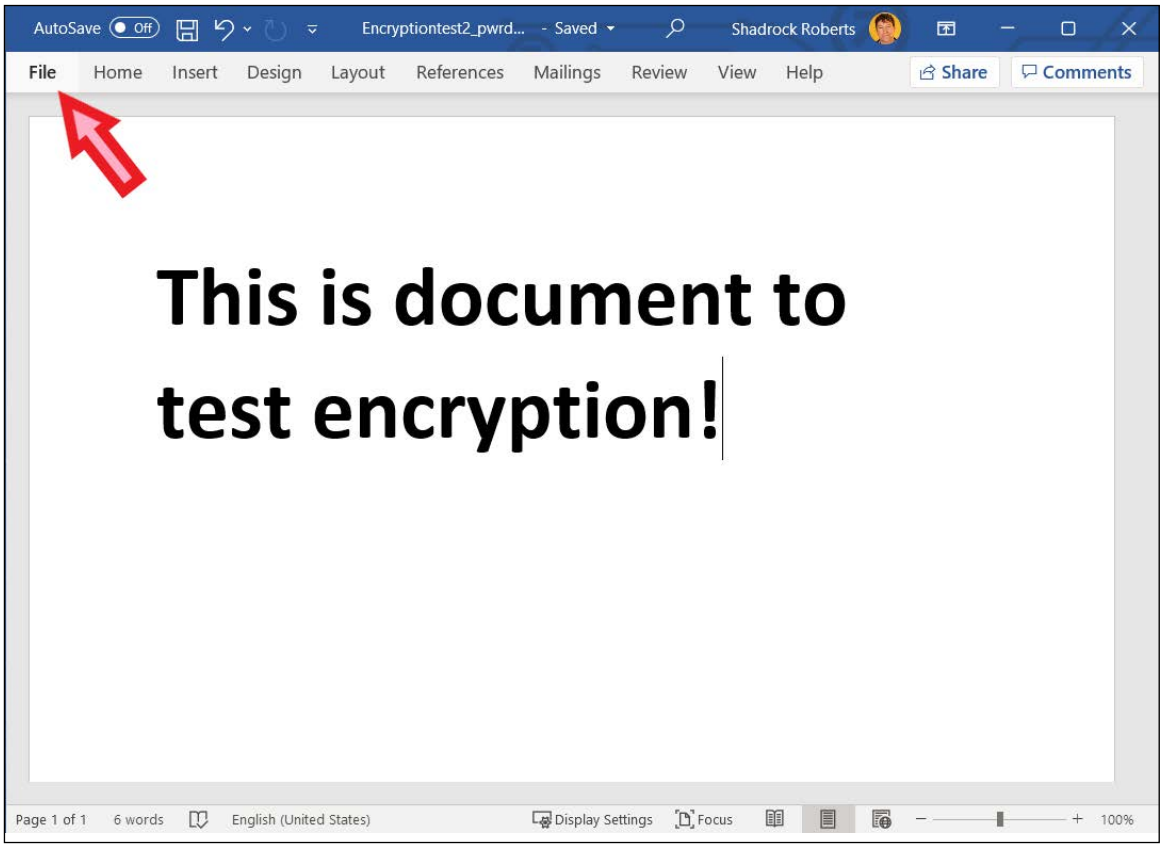
Принципи

- Використовуйте затверджені системи Mercy Corps для зашифрованої передачі та зберігання даних (наприклад, Microsoft SharePoint або Google Диск). Якщо сумніваєтеся, зверніться за порадою до місцевої IT-команди.
- Шифруйте чутливі дані на всіх етапах їх збору, використання, передачі та зберігання.
- Використовуйте надійні паролі та не використовуйте паролі повторно. Списки паролів циркулюють в інтернеті та полегшують доступ до кількох ваших облікових записів або файлів тому, хто має один з ваших паролів! Можливо, ви захочете скористатися менеджером паролів, наприклад Lastpass. Однак менеджери паролів можуть бути вразливими до кібератак фальшивих додатків, тому вкрай важливо, щоби менеджери паролів використовувалися як частина ширшого підходу до захисту даних.

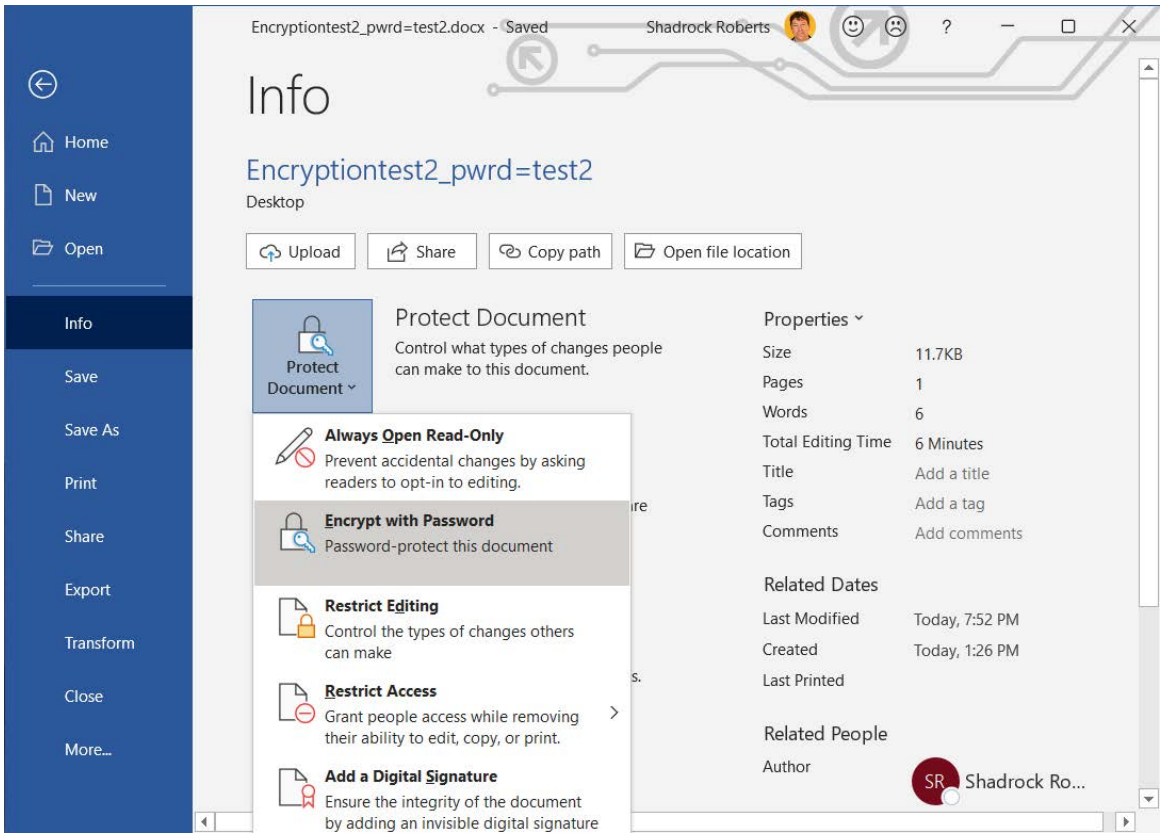
- У командному середовищі шифрування настільки надійне, наскільки надійна його найслабша ланка. Якщо навіть одна людина не використовує шифрування, дані вашої програми перебувають під загрозою. Надзвичайно важливо донести своїй команді: шифрування — це питання не лише технологій, але й зміни поведінки.
- Розберіться із законами, які регулюють шифрування у вашій країні. Місцеві закони в ряді країн (зокрема Судані, Ємені та Пакистані) накладають обмеження на програмне забезпечення для шифрування. Якщо сумніваєтеся, зверніться до місцевої IT-команди за порадою: як правило, вони співпрацюватимуть із вами, щоби забезпечити належне шифрування жорстких дисків ваших комп'ютерів за допомогою Intune.

Інструкції

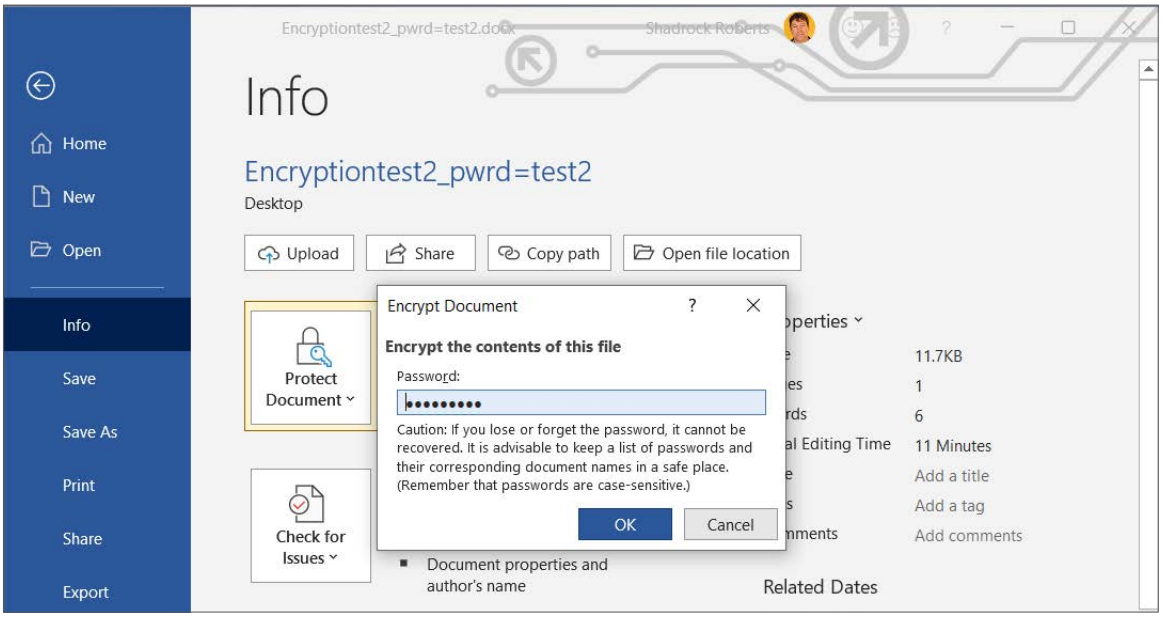
1 Відкрийте файл Word, Excel або PowerPoint, який потрібно зашифрувати, і виберіть меню **"Файл"**.



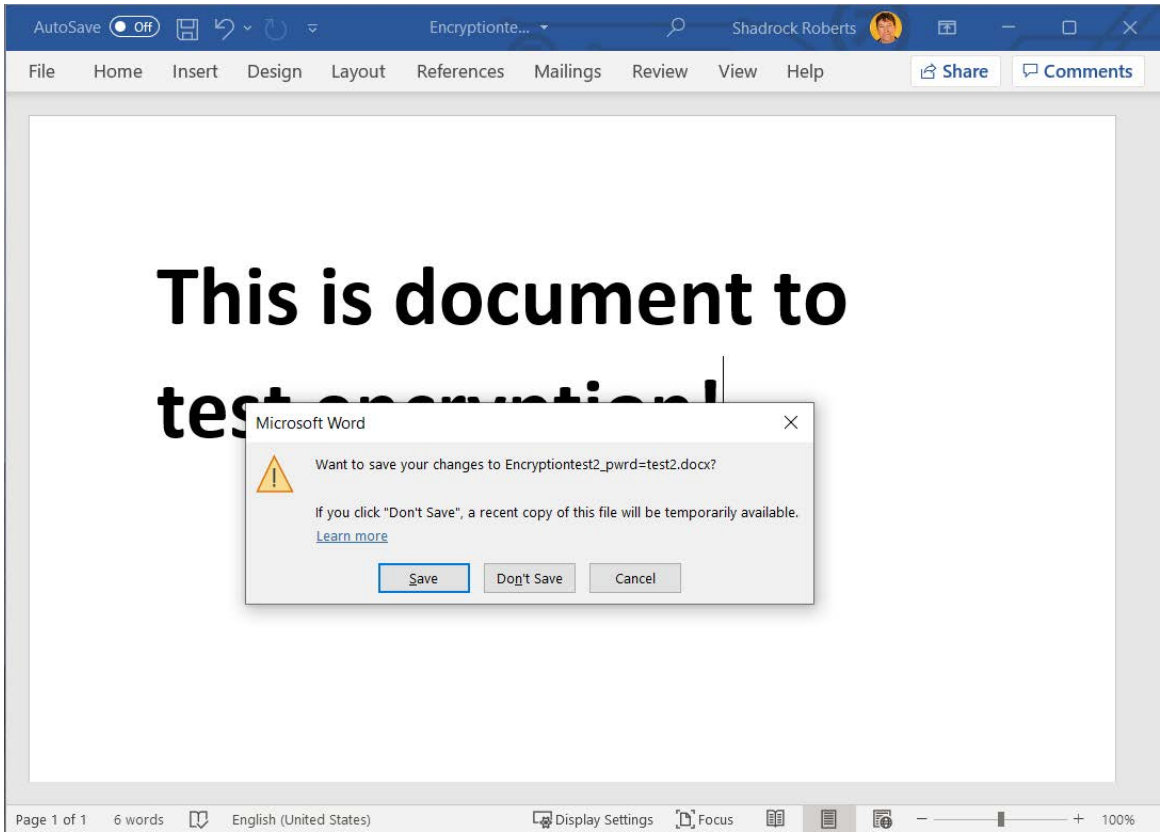
2 Перейдіть до **"Інформація"** > **"Захистити документ"** > **"Шифрування паролем"**.



3 Введіть пароль, натисніть **OK**, а потім введіть його ще раз, щоби підтвердити.



4 Збережіть файл, щоби переконатися, що пароль діє.



Тепер ви можете поділитися файлом і паролем з тими, хто потребує доступу. Найкраще розміщувати файл на хмарному сервісі, затвердженому Mercy Corps, зокрема G Suite або SharePoint. Не забудьте надіслати посилання на файл і посилання на пароль окремо. Наприклад, ви можете поділитися файлом за допомогою Google Диска (**див. розділ "Спільне використання файлів"**) і створити повідомлення про те, що файл був переданий через Google, а потім переслати пароль на електронну пошту колеги.

Додаткова підтримка

- "Довідник про дані для початківців" від Electronic Cash Transfer Learning Action Network містить низку порад щодо шифрування (див. листок порад №5).
- Electronic Frontier Foundation більш детально розглядає різні форми шифрування.
- "Довідник спеціаліста із сучасного розвитку" від Engine Room містить розділ про керування даними, в якому наводяться додаткові думки високого рівня про шифрування.

КОНТАКТИ

ХІЗЕР ЛАВ (HEATHER LOVE)
Директор із глобального захисту та конфіденційності даних | IT
hlove@mercycorps.org

ШЕДРОК РОБЕРТС (SHADROCK ROBERTS)
Спеціаліст із захисту даних | IT
shroberts@mercycorps.org

Про Mercy Corps

Mercy Corps — провідна всесвітня організація, яка спирається на віру в те, що кращий світ можливий. Під час катастроф і негод, у більш ніж 40 країнах по всьому світу ми співпрацюємо, щоби ввести сміливі рішення в дію, допомагаючи людям перемогти негаразди й побудувати сильніші громади зсередини.
І зараз, і на майбутнє.

MERCY CORPS

Всесвітня штаб-квартира
45 SW Ankeny Street
Портленд, Орегон 97204
888 842 0842
mercycorps.org

Європейська штаб-квартира
40 Sciences
Единбург EH9 1NJ
Шотландія, Великобританія
+44 131 662 5160
mercycorps.org.uk