Korzystanie z danych „wrażliwych”

Wytyczne dotyczące przetwarzania danych wrażliwych

Spis treści

Uzasadnienie

Większość programów i innych działań Mercy Corps gromadzi pewnego rodzaju dane osobowe osób, którym służymy i z którymi pracujemy, a wiele z nich gromadzi również informacje o osobach, które można sklasyfikować jako wrażliwe. Gromadzenie danych wrażliwych jest niezbędne do wykonywania naszej pracy i służenia uczestnikom programu oraz społecznościom, w których działamy. W związku z tym, gdy gromadzimy i wykorzystujemy dane wrażliwe, niezwykle ważne jest podjęcie wszelkich niezbędnych kroków w celu zapewnienia ochrony tych danych. Brak ochrony danych wrażliwych może prowadzić do poważnych szkód dla osoby, której dane dotyczą, w tym m.in. do dyskryminacji i zagrożenia bezpieczeństwa.

Zakres

Niniejsze wytyczne mają zastosowanie do wszystkich przypadków przetwarzania danych wrażliwych w całej agencji. Dotyczą one danych wrażliwych gromadzonych w celach programowych i operacyjnych oraz wszelkich innych sytuacji, w których występują dane wrażliwe. Niniejszy dokument szczegółowo określa niezbędne kroki, jakie należy podjąć w każdym przypadku przetwarzania danych wrażliwych.

Czym są dane wrażliwe i dlaczego różnią się od innych rodzajów danych osobowych?

Dane wrażliwe to zazwyczaj dane takie jak profil kulturowy, orientacja seksualna, dane biometryczne i genetyczne dotyczące zdrowia danej osoby. Są to dane, których niewłaściwe ujawnienie, dostęp lub udostępnienie może:

- wyrządzić szkody (takie jak sankcje, dyskryminacja i zagrożenia dla bezpieczeństwa) osobom, w tym źródłu informacji oraz innym możliwym do zidentyfikowania osobom lub grupom;
- mieć negatywny wpływ na zdolność organizacji do prowadzenia działalności lub na postrzeganie tej organizacji przez opinię publiczną.

Przykład 1:

Program jest realizowany w pewnej społeczności i w trakcie jego trwania kilku uczestników ujawnia, że są nosicielami wirusa HIV. Informacje te zostają przypadkowo udostępnione starszym członkom społeczności, co może prowadzić do znacznych szkód, a nawet zagrożenia fizycznego dla uczestników programu.

Przykład 2:

W biurze planowana jest uroczystość i zbierane są informacje o wymaganiach żywieniowych członków zespołu. Kilku członków zespołu zgłosiło zapotrzebowanie na posiłki koszerne lub przygotowane zgodnie z zasadami Halal. Cały zespół ma dostęp do arkusza z informacjami o tym, którzy członkowie zespołu mają szczególne wymagania żywieniowe. Niektórzy członkowie zespołu nie podzielili się informacjami na temat wyznawanej przez siebie religii, ponieważ obawiają się dyskryminacji.

Dane wrażliwe należy traktować z większą ostrożnością, ponieważ ich gromadzenie i wykorzystywanie może w większym stopniu naruszać podstawowe prawa lub wolności osób fizycznych lub powodować znaczne szkody, w tym dyskryminację lub zagrożenie fizyczne, jeżeli zostaną one niewłaściwie wykorzystane.

W ogólnym rozporządzeniu o ochronie danych (RODO) zdefiniowano szereg typów danych zaliczanych do kategorii danych szczególnie chronionych i określono szczegółowe warunki przetwarzania tych typów danych. Należy jednak pamiętać, że w niektórych kontekstach dane, które nie mieszczą się w standardowej kategorii danych szczególnie chronionych, mogą nadal być szczególnie chronione ze względu na szczególny kontekst. Dla celów niniejszych wytycznych dane tego typu określane będą jako dane wrażliwe kontekstowo.

Niniejsze wytyczne zostały opracowane jako uzupełnienie Polityki Odpowiedzialnego Zarządzania Danymi oraz Polityki Zarządzania Programami Mercy Corps (która obejmuje również Politykę MEL agencji) i mają zastosowanie do gromadzenia danych wrażliwych we wszystkich kontekstach, w tym, między innymi, danych dotyczących centrali, programów i MEL.

Definicje kluczowych pojęć

- **Dane operacyjne Mercy Corps** – Każda jednostka informacji, składająca się z liter, liczb, symboli, obrazów, nagrań wideo i głosu, współrzędnych geoprzestrzennych lub identyfikatorów lokalizacji, map lub dowolnej ich kombinacji, przetwarzana przez Mercy Corps. Może to obejmować między

innymi dane dotyczące członków zespołu Mercy Corps, dostawców, darczyńców lub partnerów. Dane istnieją zarówno w postaci cyfrowej, jak i fizycznej.

- **Dane wrażliwe** – Informacje te są często wykorzystywane jako podstawa do kierowania działań do konkretnej grupy lub osoby. Typowe przykłady stanowią: rasa, religia, poglądy polityczne, orientacja seksualna, zdrowie lub dane biometryczne.

  Na potrzeby niniejszej notatki dane wrażliwe obejmują „dane wrażliwe szczególnej kategorii", jak określono w RODO, oraz „dane wrażliwe kontekstowo".

- **Dane wrażliwe kategorii specjalnej** – RODO określa szczegółowe wymogi dotyczące przetwarzania wszystkich danych wrażliwych kategorii specjalnej, które muszą być spełnione. RODO definiuje dane wrażliwe szczególnej kategorii jako:

  - dane osobowe ujawniające pochodzenie rasowe lub etniczne;
  - dane osobowe ujawniające poglądy polityczne;
  - dane osobowe ujawniające przekonania religijne lub filozoficzne;
  - dane osobowe ujawniające przynależność do związków zawodowych;
  - dane genetyczne;
  - dane biometryczne (tam, gdzie są one wykorzystywane do celów identyfikacji);
  - dane dotyczące stanu zdrowia;
  - dane dotyczące życia seksualnego danej osoby; oraz
  - dane dotyczące orientacji seksualnej danej osoby

- **Dane wrażliwe kontekstowo** – dane, które nie należą do kategorii danych wrażliwych określonych w RODO, ale które ze względu na kontekst, w jakim są przetwarzane, mają charakter danych wrażliwych i których ujawnienie mogłoby wyrządzić znaczną szkodę osobie, której dane dotyczą.

- **Naruszenie danych osobowych** – Naruszenie ochrony danych osobowych można szeroko zdefiniować jako incydent bezpieczeństwa, który wpłynął na poufność, integralność lub dostępność danych osobowych. Krótko mówiąc, naruszenie ochrony danych osobowych będzie miało miejsce zawsze wtedy, gdy jakiekolwiek dane osobowe zostaną utracone, zniszczone, uszkodzone lub ujawnione; gdy ktoś uzyska dostęp do tych danych lub przekaże je dalej bez odpowiedniego upoważnienia; lub gdy dane staną się niedostępne, na przykład gdy zostaną zaszyfrowane przez oprogramowanie ransomware albo przypadkowo utracone lub zniszczone.

- **Dane związane z programem** – Każda jednostka informacji, składająca się z liter, liczb, symboli, obrazów, nagrań wideo i głosowych lub dowolnej ich kombinacji, dotycząca uczestników programu, jego realizacji i wyników. Dane istnieją zarówno w postaci cyfrowej, jak i fizycznej.

- **Polityka Odpowiedzialnego Korzystania z Danych Mercy Corps** – Polityka agencji, której celem jest określenie zasad przejrzystego, bezpiecznego i odpowiedzialnego korzystania z danych osobowych w całej agencji oraz uwzględnianie tych zasad w naszej codziennej pracy.

- **Świadoma zgoda** – Proces uzyskiwania dobrowolnej zgody na gromadzenie danych dowolnego rodzaju, oparty na jasnej ocenie i zrozumieniu faktów, implikacji i konsekwencji każdego zaangażowania ze strony uczestników. Zgoda ta może być wyrażona w formie oświadczenia pisemnego lub ustnego, bądź przez wyraźne działanie potwierdzające. Zgodę należy uzyskać w momencie gromadzenia Danych osobowych lub tak szybko, jak to będzie możliwe po tym fakcie.

- **Wyraźna zgoda** – Wyraźna zgoda wymaga bardzo jasnego i konkretnego oświadczenia o wyrażeniu zgody. Należy rejestrować, kiedy i w jaki sposób uzyskano zgodę oraz co dokładnie powiedziano osobom, których dane dotyczą, gdy zgodę uzyskano. Wyraźna zgoda musi określać charakter danych kategorii specjalnej i powinna być odrębna od wszelkich innych zgód, o które się ubiega.

- **Usuwanie tożsamości** – Wszelkie działania lub metody przetwarzania danych, które mają na celu uniemożliwienie bezpośredniego i/lub pośredniego ujawnienia tożsamości uczestnika lub innej osoby. Przykładowe typy: Anonimizacja (tj. usunięcie pewnych ilości danych osobowych lub zastosowanie zakresu wartości do pewnych zestawów danych osobowych) oraz pseudonimizacja (tj. przetwarzanie danych osobowych w taki sposób, że nie można ich już przypisać do konkretnej osoby lub grupy osób, których dane dotyczą, bez użycia dodatkowych informacji, takich jak unikalne identyfikatory lub skrypty).

- **Informacje umożliwiające identyfikację osoby (PII)** – Informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dotyczą dane”); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. Są one ściśle związane z **informacjami umożliwiającymi identyfikację demograficzną (DII)**, które mogą być wykorzystane do identyfikacji społeczności lub odrębnej grupy geograficznej, etnicznej, religijnej, ekonomicznej lub politycznej.

- **Przechowywane w bezpieczny sposób** – Dostęp do danych mają tylko niezbędni członkowie zespołu Mercy Corps; podejmowane są kroki mające na celu zapobieganie kradzieży i niewłaściwemu wykorzystaniu danych. Przechowywane w bezpieczny sposób – Dostęp do danych mają tylko niezbędni członkowie zespołu Mercy Corps; podejmowane są kroki mające na celu zapobieganie kradzieży i niewłaściwemu wykorzystaniu danych. Plik jest bezpiecznie przechowywany, gdy:
  - znajduje się one na platformie, która posiada / spełnia surowe normy bezpieczeństwa, ochrony danych i prywatności
  - dostęp jest ograniczony tylko do wymaganych stron
  - dostęp jest regularnie sprawdzany i w razie potrzeby dostosowywany.

- Dodatkowe wymogi zostały określone dla programów Mercy Corps w nowo przyjętej Polityce MEL, w szczególności Standard 9, który wymaga od wszystkich programów zapewnienia praktyk

bezpiecznego obchodzenia się z danymi, zgodnie z Polityką odpowiedzialnego zarządzania danymi i wymogami darczyńców.

- **Niezbędni członkowie zespołu Mercy Corps** – Członkowie zespołu, którzy potrzebują dostępu do zidentyfikowanych informacji w celu wykonywania zadań związanych z ich pracą, takich jak zaspokajanie potrzeb uczestników programu i realizacja zadań programu

- **Osoba, której dotyczą dane** – Każda osoba fizyczna, od której i o której gromadzone są dane bezpośrednio, pośrednio lub za pośrednictwem strony trzeciej, i którą można zidentyfikować, bezpośrednio lub pośrednio, w szczególności poprzez odniesienie do danych osobowych.

- **Ochrona danych** – Zabezpieczanie i zapobieganie nieupoważnionemu dostępowi do informacji umożliwiających identyfikację osób (PII), informacji umożliwiających identyfikację demograficzną (DII) oraz innych wrażliwych danych dotyczących osób lub grup w całym cyklu danych dotyczących zarządzania programem lub projektem lub po zakończeniu programu lub projektu. Polityka Odpowiedzialnego Zarządzania Danymi Mercy Corps określa wymagania dotyczące ochrony danych, a agencja podlega również innym ramom prawnym / regulacyjnym, takim jak Ogólne Rozporządzenie Unii Europejskiej o Ochronie Danych (RODO).

Więcej definicji związanych z odpowiedzialnym korzystaniem z danych znaleźć można w dokumencie Definicje odpowiedzialnego korzystania z danych.

Planowanie

- Należy rozważyć, jakie rodzaje danych będą gromadzone, i udokumentować to na etapie planowania projektu, w Ocenie wpływu na prywatność (PIA).

- Jeżeli plan przewiduje gromadzenie i/lub dokumentowanie i/lub przechowywanie wszelkiego rodzaju danych wrażliwych, należy zwrócić szczególną uwagę na to, jak i dlaczego dane te są wykorzystywane. Należy rozważyć, czy gromadzenie tych danych jest niezbędne do osiągnięcia wymaganych rezultatów programu lub projektu, czy też wystarczyłby alternatywny rodzaj danych. Dane wrażliwe powinny być gromadzone tylko wtedy, gdy jest to konieczne. Należy pamiętać, że gromadzenie danych wrażliwych, jeżeli jest prawidłowo realizowane, jest kosztownym procesem. Poprzez zmniejszenie obciążenia związanego z niepotrzebnym gromadzeniem danych, umożliwiasz zespołom zaoszczędzenie czasu i zasobów na inne niezbędne prace. W przypadku stwierdzenia, że dane PII są niezbędne, nie należy stosować skrótów. Jeżeli zasoby przeznaczone na gromadzenie danych wrażliwych i zarządzanie nimi są niewystarczające, aby robić to prawidłowo, ponownie rozważ ryzyko, jakie mogą powodować dla społeczności, z którymi współpracujemy.

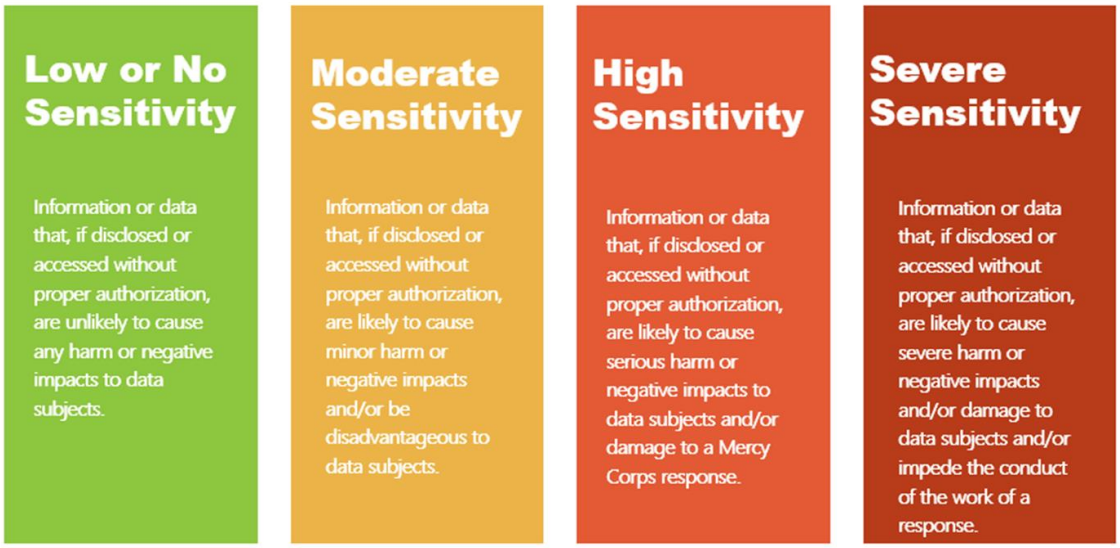
- Rozważ, jakie technologie będą wykorzystywane do gromadzenia i przechowywania danych. Stosowane technologie muszą obejmować odpowiednie zabezpieczenia w zakresie gromadzenia informacji wrażliwych.

- Ogólnie rzecz biorąc, im bardziej wrażliwe dane, tym więcej zabezpieczeń należy wprowadzić. Dane wrażliwe będą zazwyczaj miały stopień wrażliwości „wysoki” lub „poważny” (patrz ilustracja 1). Ponadto im więcej zbiorów danych jest gromadzonych, tym większe jest ryzyko i tym więcej zabezpieczeń należy wprowadzić. Przykłady zabezpieczeń obejmują między innymi:

    - Szyfrowanie;
    - Pseudonimizację ;
    - Dysocjację;
    - Przechowywanie akt papierowych w zamykanych szafach o ograniczonym dostępie;
    - Przechowywanie plików na serwerach Mercy Corps z poziomami ochrony;
    - Ograniczenie dostępu do urządzeń Mercy Corps tylko do osób, które muszą mieć do nich dostęp, aby wykonywać swoje obowiązki służbowe;
    - Dopilnowanie, aby urządzenia takie jak laptopy były zablokowane, gdy nie są używane;
    - W przypadku danych przestrzennych – randomizowanie lub agregowanie punktów GPS.

- Należy jasno określić, jaka podstawa prawna przetwarzania danych wrażliwych będzie stosowana i odpowiednio ją zaplanować.
- Wymogi dotyczące sprawozdawczości w umowach o dotację muszą być zgodne z zasadą nieszkodzenia (np. nie oczekuje się, że w ramach programu gromadzone będą mogąc zagrażać bezpieczeństwu uczestników) oraz wyraźnie określać zobowiązania i umowy dotyczące platform udostępniania danych, procesów z darczyńcami, partnerami i innymi interesariuszami, z uwzględnieniem wymogów dotyczących identyfikacji i anonimizacji.
- Protokół bezpieczeństwa danych na poziomie programu jest częścią Planu Technologicznego MEL (Standard 6) i zawiera informacje na temat danych członków zespołu, w tym poziomy uprawnień i protokoły dla członków zespołu MC i członków zespołu spoza MC.
- Jeżeli dla celów operacyjnych Mercy Corps gromadzone są dane wrażliwe, należy zaplanować i przedstawić w zarysie kwestie związane z danymi, w tym poziomy uprawnień i protokoły.
- Należy zastanowić się i uzasadnić, jak długo należy przechowywać dane (okres przechowywania) - zależy to od powodów ich gromadzenia, wymogów prawnych, wymagań darczyńców oraz zasad przechowywania dokumentacji programu MC.
- Należy wdrożyć proces niszczenia danych po upływie okresów przechowywania.

Ilustracja 1:



Planowanie gromadzenia danych

- Ocenę wpływu na prywatność przeprowadza się w celu identyfikacji i zarządzania ryzykiem związanym z prywatnością danych, związanym z wszelkimi nowymi działaniami, takimi jak nowe programy, technologie czy zasady. Jeżeli mają być gromadzone dane wrażliwe, muszą one być sprawdzone przez kompetentną osobę. Może to być zespół ds. ochrony danych i prywatności, inspektor ochrony danych lub zgodnie z polityką MEL (Minimalny standard nr 9 – Prywatność i bezpieczeństwo danych):
    - Osoba odpowiedzialna – Dyrektor Krajowy lub Dyrektor ds. Programów i Kierownik Programów lub Szef Strony
    - Zalecana osoba odpowiedzialna – lider programu MEL / lider zarządzania wiedzą

- Należy przeprowadzić Ocenę informacji wrażliwych (SIA) powiązaną z procedurą PIA. Powinna ona dokumentować wszystkie dodatkowe zabezpieczenia stosowane w odniesieniu do danych wrażliwych.

- Jeżeli podstawą prawną jest zgoda, świadoma zgoda wymaga, by osoby, których dane dotyczą, zostały poinformowane prostym językiem o następujących kwestiach:

    - Jakie dane są gromadzone i dlaczego są one wymagane;

    - Komu będą one udostępniane, w tym partnerom zewnętrznym i darczyńcom;

    - Czy dane będą udostępniane w skali międzynarodowej;

    - Jak długo dane będą przechowywane.

- Należy odnotować, kiedy i w jaki sposób uzyskano zgodę oraz co powiedziano osobie, której dane dotyczą. Na etapie planowania należy uwzględnić szablon informacji, jakie zostaną przekazane osobom, których dane dotyczą, w celu uzyskania zgody

Gromadzenie danych

- Dla każdego przypadku gromadzenia danych sporządza się protokół gromadzenia danych, który obejmuje:
    - Dodatkowe zabezpieczenia danych wrażliwych;
    - W stosownych przypadkach udokumentowane instrukcje dotyczące gromadzenia, czyszczenia, przeglądu i usuwania danych identyfikacyjnych;
    - Instrukcje dotyczące potencjalnych naruszeń bezpieczeństwa danych w odniesieniu do wszystkich gromadzonych danych ilościowych i jakościowych (np. zagubione lub skradzione urządzenia, naruszone loginy itp.);
    - Instrukcje dotyczące wykorzystania i ochrony formularzy papierowych podczas gromadzenia danych;
    - Wyrywkowe kontrole i monitorowanie stopnia, w jakim osoby gromadzące dane przestrzegają protokołów dotyczących bezpieczeństwa i ochrony.
- Wszystkie powyższe elementy powinny być powiązane z oceną SIA

Przechowywanie danych

- Pliki zawierające informacje wrażliwe muszą być zastrzeżone dla członków zespołu, którzy potrzebują dostępu do tych informacji w celu wykonania niezbędnych zadań, a systematyczne usuwanie tożsamości z informacji wrażliwych jest przeprowadzane przed połączeniem ich z TolaData lub udostępnieniem stronie trzeciej, jeżeli jest to właściwe. Standard 8 polityki MEL zawiera dodatkowe wskazówki dotyczące najlepszych praktyk w zakresie archiwizacji i przechowywania danych MEL.
- Dane są przechowywane w miejscu, które jest zgodne ze wszystkimi odpowiednimi zasadami Mercy Corps (np. Polityka Odpowiedzialnych Danych, Akceptowalne Użytkowanie).
- Dane wrażliwe muszą być przechowywane nie dłużej niż jest to konieczne. Po upływie okresów przechowywania dane muszą zostać bezpiecznie zniszczone lub w pełni zanonimizowane.
- Okresy przechowywania muszą być udokumentowane i uzasadnione.
- Pamiętaj - dane mogą być również przechowywane w mobilnych systemach gromadzenia danych. Wszystkie wyżej wymienione kwestie związane z przechowywaniem danych dotyczą także mobilnych systemów gromadzenia danych.

Analiza danych

- Istnieje protokół udostępniania danych konsultantom, zespołom centrali, partnerom, interesariuszom, obejmujący m.in. umowy o udostępnianiu danych, zgody krajowego MEL, role i obowiązki itp.

- Umowy o zachowaniu poufności (NDA) są podpisywane przez wszystkich konsultantów przed uzyskaniem dostępu do jakichkolwiek zbiorów danych będących własnością Mercy Corps.

Przekazywanie danych darczyńcy, partnerowi lub innej stronie trzeciej (jeżeli dotyczy)

- Dane nieprzetworzone pozbawiane są cech umożliwiających identyfikację, a przed przekazaniem są sprawdzane pod kątem zgodności z zasadami nieszkodzenia.
- Danych wrażliwych nie wolno udostępniać osobom trzecim, które nie zostały wymienione w procesie uzyskiwania świadomej zgody.
- Danych wrażliwych nie wolno udostępniać osobom trzecim, chyba że zawarto umowę o udostępnianiu danych.
- Do udostępniania dokumentów należy używać wyłącznie autoryzowanych systemów organizacyjnych, takich jak Google Drive lub Microsoft Sharepoint, a nie platform udostępniania innych firm.

Często zadawane pytania

Aby zapewnić zgodność z wymogami dotyczącymi różnorodności, prosimy członków zespołu o podanie swojego statusu etnicznego w formularzach podań o pracę - czy muszę coś z tym zrobić?

Tak, dane dotyczące pochodzenia rasowego lub etnicznego są uważane za wrażliwe dane osobowe, dlatego należy postępować zgodnie z wytycznymi dotyczącymi danych wrażliwych i stosować dodatkowe zabezpieczenia w odniesieniu do tych danych.

Co się stanie, jeżeli ja lub członek zespołu przypadkowo, nieumyślnie udostępnimy dane wrażliwe? Jakie działania zaradcze można wtedy podjąć?

Po stwierdzeniu przypadkowego udostępnienia danych osobowych należy natychmiast zaprzestać ich udostępniania. Może to oznaczać zwrócenie się do przypadkowego odbiorcy z prośbą o usunięcie wszelkich kopii danych, odebranie przypadkowemu odbiorcy dostępu do danych, usunięcie danych z Internetu lub podjęcie innych kroków w zależności od potrzeb.

Przypadkowe lub niezamierzone udostępnienie danych osobowych jest traktowane jako naruszenie danych i należy niezwłocznie powiadomić o tym fakcie **it-security@mercycorps.org** zgodnie z Planem reagowania na incydenty. Należy jak najszybciej przekazać jak najwięcej informacji o charakterze udostępnianych danych.

Co mam zrobić, gdy widzę, że członek zespołu celowo udostępnia poufne dane osobie, która nie powinna mieć do nich dostępu?

Umyślne udostępnienie danych wrażliwych osobie nieupoważnionej jest niezwykle poważne, ponieważ może prowadzić do poważnych szkód dla osoby, której dane dotyczą, oraz dla agencji. Jeżeli zauważysz, że członek zespołu celowo dzieli się w ten sposób poufnymi informacjami, powinieneś niezwłocznie zgłosić to kierownikowi programu, dyrektorowi regionalnemu lub swojemu dyrektorowi.

Również udostępnienie danych wrażliwych osobom, które nie powinny mieć do nich dostępu, stanowi naruszenie ochrony danych i powinno być niezwłocznie zgłoszone na adres **it-security@mercycorps.org** zgodnie z Planem reagowania na incydenty. Należy jak najszybciej przekazać jak najwięcej informacji o charakterze udostępnianych danych.

W jaki sposób program decyduje o tym, kto powinien/nie powinien mieć dostępu do danych wrażliwych?

Dostęp do danych wrażliwych powinny mieć tylko osoby, którym jest on niezbędny do pełnienia ich funkcji. O ile to możliwe, dane wrażliwe należy zawsze maskować przed ich udostępnieniem. Typowe przykłady maskowania to anonimizacja lub pseudonimizacja.

Co to są dane zdysocjowane?

Dane zdysocjowane to dane, które zostały całkowicie i nieodwracalnie odłączone od osoby, której dane dotyczą, tak że nie ma już możliwości ponownego powiązania tych danych z osobą, której dane dotyczą. Dane zdysocjowane to rodzaj anonimizacji danych.

Czy należy uruchomić alerty dotyczące elektronicznego zbioru danych, jeżeli dostęp do niego uzyskała osoba nieupoważniona?

Jeżeli możliwe jest uruchamianie alertów w przypadku nieuprawnionego dostępu, należy je zawsze włączać, jednak nie wszystkie platformy elektroniczne mają taką możliwość. Sprawdź ustawienia systemowe swojej platformy i jeżeli to możliwe, uruchom alerty.

Czy członkowie zespołu powinni używać urządzeń osobistych do gromadzenia lub przechowywania informacji wrażliwych? Jeżeli tak, to jakie zabezpieczenia należy zapewnić?

Urządzenia osobiste nie powinny być wykorzystywane do gromadzenia lub przechowywania danych osobowych, w tym informacji o uczestnikach, *chyba że zainstalowano odpowiednie oprogramowanie do zarządzania urządzeniami,* a korzystanie z urządzeń osobistych zostało odnotowane w PIA projektu. Do gromadzenia danych uczestników nigdy nie wolno używać urządzeń osobistych bez wyraźnej zgody kierownika programu. Urządzeń osobistych nie należy używać do gromadzenia lub przechowywania informacji wrażliwych.

Czy darczyńca może skontrolować, w jaki sposób obchodzę się z danymi wrażliwymi?

Tak, wielu darczyńców wymaga wewnętrznych, a także zewnętrznych audytów jakości danych i ocen jakości danych. Jednym z aspektów tych ocen jest ocena systemu MEL pod kątem wstrząsów, ingerencji i bezpieczeństwa, zwłaszcza jeżeli program przewiduje gromadzenie danych wrażliwych.

Czy mogę połączyć listy uczestników z TolaData jako dowód?

Listy uczestników (np. listy obecności na szkoleniach itp.) mogą być powiązane jako dowody, ponieważ te dowody powinny być umieszczone i przechowywane poza TolaData, a zatem tylko określone osoby będą miały dostęp do tych dowodów, zgodnie z uprawnieniami w tym zewnętrznym miejscu przechowywania. Należy rozważyć, czy jakikolwiek rodzaj dowodów powiązanych z TolaData wymaga podania danych osobowych. Jest bardzo mało prawdopodobne, aby konieczne było zamieszczanie informacji wrażliwych.

Skąd mam wiedzieć, czy dostawcy lub platformy technologii gromadzenia lub przechowywania danych są zgodne z wymogami dotyczącymi danych wrażliwych?

Istniejące platformy gromadzenia i przechowywania danych w pakiecie MEL Tech Suite są już zgodne z wymogami dotyczącymi danych wrażliwych, pod warunkiem, że są odpowiednio skonfigurowane do stosowania zabezpieczeń i protokołów opisanych w niniejszym dokumencie. Jeżeli ma być wykorzystywana platforma spoza pakietu MEL Tech Suite, należy przeprowadzić ocenę wpływu na prywatność (PIA), aby ocenić, czy można ją uznać za zgodną z wymogami dotyczącymi danych wrażliwych. Jeżeli chodzi o ocenę dostawcy technologii i jego gotowości do zachowania zgodności z Polityką odpowiedzialnego korzystania z danych oraz wymogami dotyczącymi danych wrażliwych, PIA jest ponownie najlepszym narzędziem do określenia, czy jego praktyki zostaną uznane za zgodne z przepisami.

Jak rozpoznać, czy dane są danymi osobowymi czy wrażliwymi?

Jeżeli przetwarzasz dane, które należą do którejś ze specjalnych kategorii danych wrażliwych określonych w RODO (patrz **Dane wrażliwe kategorii specjalnych** powyżej), zawsze będą to dane wrażliwe. Jeżeli z konkretnego kontekstu wynika, że dane należą do kategorii „w poważnym stopniu wrażliwe” (patrz ilustracja 1 powyżej), należy je również zaklasyfikować jako dane wrażliwe.

Powiązane dokumenty:

Zgoda

Narzędzie MEL: Szablon świadomej zgody (dla uczestników wywiadów)

Wytyczne dotyczące świadomej zgody na udostępnianie danych CARM

Wytyczne w zakresie zdalnego MERL dot. COVID-19

Szyfrowanie

Korzystanie z Ona.io w Mercy Corps: Szyfrowanie formularzy i danych wrażliwych

Dane biometryczne

Biometrics @ Mercy Corps: Primer wewnętrzny

Przewodniki ogólne

- Zestaw narzędzi związanych z odpowiedzialnym korzystaniem z danych - przewodnik dla osób odpowiedzialnych za wypłatę gotówki i wydawanie bonów - https://www.calpnetwork.org/wp-content/uploads/2021/03/Data-Responsibility-Toolkit_A-guide-for-Cash-and-Voucher-Practitioners.pdf
- Zestaw startowy danych ELAN dla pracowników terenowych organizacji humanitarnych v https://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf
- Podręcznik ICRC dotyczący ochrony danych w akcjach humanitarnych: https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

Usuwanie tożsamości z danych

Wytyczne USDA dotyczące sprawdzania informacji umożliwiających identyfikację osób (PII) w ocenach projektów

„Identyfikacja na potrzeby publikacji danych" Poverty Action Lab

Generowanie niepowtarzalnych kodów dla uczestników programu lub innych osób, których dane dotyczą

Wersja robocza wytycznych T4D

Oceny

Ocena wpływu na prywatność (PIA) - szablon-

Ocena wpływu na prywatność (PIA) - wskazówki-

Ocena informacji wrażliwych (SIA)