استخدام البيانات "الحساسة"

إرشادات معالجة البيانات الحساسة

جدول المحتويات

الأساس المنطقي

تجمع غالبية برامج منظمة Mercy Corps وأنشطتها الأخرى نوعًا من المعلومات الشخصية حول الأفراد الذين نخدمهم ونعمل معهم، كما تجمع العديد منها معلومات حول الأفراد تُصنَّف بكونها حساسة. يُعد جمع البيانات الحساسة أمرًا ضروريًا بالنسبة لنا لتنفيذ عملنا وخدمة المشاركين في البرامج ومجتمعاتهم التي نعمل فيها؛ ولذا، نظرًا لأننا نجمع البيانات الحساسة ونستخدمها، يكون من المهم للغاية أن يتم اتخاذ جميع الخطوات اللازمة لضمان حماية هذه البيانات. ويمكن للإخفاق في حماية البيانات الحساسة أن يؤدي إلى أضرار جسيمة لصاحب البيانات بما في ذلك على سبيل المثال لا الحصر التمييز والتهديدات الأمنية ضده.

النطاق

تنطبق هذه الإرشادات على جميع عمليات معالجة البيانات الحساسة على مستوى الوكالة بأكملها. وهي تنطبق أيضًا على البيانات الحساسة التي تم جمعها لأغراض برامجية وأغراض تشغيلية وأي موقف آخر حيث توجد بيانات حساسة. توضح هذه الوثيقة بالتفصيل الخطوات اللازم اتخاذها عند إجراء معالجة لبيانات حساسة.

ما هي البيانات الحساسة ولماذا تختلف عن الأنواع الأخرى من البيانات الشخصية؟

تكون عادةً البيانات الحساسة عبارة عن بيانات مثل المعلومات التعريفية الثقافية للفرد وتوجهه الجنسي وبياناته الصحية وبياناته البيومترية وبياناته الجينية. وهي تمثل أيضًا البيانات التي إذا تم الكشف عنها أو الوصول إليها أو مشاركتها بشكل غير صحيح فإنها قد تؤدي إلى ما يلي:

- إلحاق الضرر (مثل العقوبات والتمييز والتهديدات الأمنية) بشخص ما، بما في ذلك مصدر المعلومات أو الأشخاص أو المجموعات الأخرى التي يمكن تحديد هويتها؛
- التأثير سلبًا على قدرة المنظمة على تنفيذ أنشطتها أو على التصورات العامة لتلك المنظمة.

المثال 1:

يعمل أحد البرامج في المجتمع وأثناء المشروع كشف العديد من المشاركين عن إصابتهم بفيروس نقص المناعة البشرية. تتم مشاركة هذه المعلومات عن طريق الخطأ مع كبار أفراد المجتمع مما يؤدي إلى احتمال إلحاق ضرر كبير بالمشاركين في البرنامج وحتى تعريضهم لخطر جسدي جسيم.

المثال 2:

يخطط أحد المكاتب للاحتفال ويقوم بجمع المتطلبات الغذائية الخاصة بأعضاء الفريق. أشار العديد من أعضاء الفريق إلى أنهم يحتاجون إما وجبات كوشر أو حلال. تمت مشاركة جدول بيانات الذي يحدد أعضاء الفريق الذين لديهم متطلبات غذائية محددة مع الفريق بأكمله. لم يشارك بعض أعضاء الفريق دينهم لأنهم يتخوفون من التعرض للتمييز.

يجب التعامل مع البيانات الحساسة بعناية أكبر لأن جمعها واستخدامها من المرجح أن يتعارض مع الحقوق أو الحريات الأساسية للفرد، أو يتسبب في إلحاق ضرر كبير به - بما في ذلك التمييز أو الخطر الجسدي - في حالة إساءة استخدامها.

تحدد اللائحة العامة لحماية البيانات (GDPR) عددًا من أنواع البيانات المُصنَّفة على أنها بيانات حساسة من فئة خاصة وتوضح بالتفصيل شروط المعالجة المحددة لهذه الأنواع من البيانات؛ ومع ذلك، يكون من المهم ملاحظة أنه في بعض السياقات قد تظل البيانات التي تقع خارج نطاق البيانات الحساسة من فئة خاصة بيانات حساسة بسبب سياقها المحدد. لأغراض هذه المذكرة الإرشادية، ستتم الإشارة إلى هذه الأنواع من البيانات على أنها بيانات حساسة سياقيًا.

تم تصميم هذه المذكرة الإرشادية لتكملة سياسة البيانات المسؤولة الخاصة بمنظمة Mercy Corps وكذلك سياسة إدارة البرامج (التي تتضمن أيضًا سياسة المراقبة والتقييم والتعلم الخاصة بالوكالة) وهي تنطبق على جمع البيانات الحساسة في جميع السياقات، بما في ذلك على سبيل المثال لا الحصر بيانات المقر الرئيسي والبيانات البرنامجية وبيانات المراقبة والتقييم والتعلم.

تعريفات المصطلحات الرئيسية

> **البيانات التشغيلية لمنظمة Mercy Corps** - تعني أي وحدة معلومات تتكون من أحرف أو أرقام أو رموز أو صور أو فيديوهات أو تسجيلات صوتية أو إحداثيات جغرافية مكانية أو مُعرّفات مواقع أو خرائط أو أي مزائج منها تتم معالجتها من قِبل منظمة Mercy Corps. قد تشمل هذه البيانات على سبيل المثال لا الحصر البيانات المتعلقة بأعضاء فريق منظمة Mercy Corps أو المورّدين أو المانحين أو الشركاء. وهي تشمل البيانات المتاحة في شكل رقمي ومادي.

> **البيانات الحساسة** - هي المعلومات التي تُستخدم غالبًا كأساس لاستهداف مجموعة معينة أو فرد معين. ومن الأمثلة الشائعة على ذلك: العرق أو الدين أو الرأي السياسي أو التوجه الجنسي أو المعلومات الصحية أو المعلومات البيومترية.

لأغراض هذه المذكرة الإرشادية، ستتضمن البيانات الحساسة كلاً من "البيانات الحساسة من فئة خاصة" كما هو موضح في اللائحة العامة لحماية البيانات و"البيانات الحساسة سياقيًا"

> البيانات الحساسة من فئة خاصة - تنص اللائحة العامة لحماية البيانات (GDPR) على المتطلبات المحددة لمعالجة كافة البيانات الحساسة من فئة الخاصة التي يجب الوفاء بها. تُعرّف اللائحة العامة لحماية البيانات (GDPR) البيانات الحساسة من فئة خاصة على النحو التالي:

- البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني؛ أو
- البيانات الشخصية التي تكشف عن الآراء السياسية؛ أو
- البيانات الشخصية التي تكشف عن المعتقدات الدينية أو الفلسفية؛ أو
- البيانات الشخصية التي تكشف عن العضوية النقابية؛ أو
- البيانات الجينية؛ أو
- البيانات البيومترية (عند استخدامها في أغراض تحديد الهوية)؛ و
- البيانات المتعلقة بالصحة؛ و
- البيانات المتعلقة بحياة الشخص الجنسية؛ و
- البيانات المتعلقة بالتوجه الجنسي للشخص؛ و

> **البيانات الحساسة سياقيًا** - تعني البيانات التي لا تندرج تحت فئات البيانات الحساسة على النحو المحدد في اللائحة العامة لحماية البيانات (GDPR) ولكن نظرًا للسياق الذي تتم معالجتها فيه تصبح حساسة بطبيعتها وقد تُلحق ضررًا كبيرًا بصاحب البيانات إذا تم الكشف عنها.

> **انتهاك البيانات الشخصية** - يمكن تعريف انتهاك البيانات الشخصية بشكل عام بأنه حادث أمني أثر على سرية البيانات الشخصية أو سلامتها أو توفرها. وباختصار، يحدث انتهاك البيانات الشخصية عند فقدان أي بيانات شخصية أو إتلافها أو تلفها أو الكشف عنها؛ أو إذا قام شخص ما بالوصول إلى البيانات أو مررها دون إذن مناسب؛ أو في حالة عدم إتاحة البيانات، على سبيل المثال عند تشفيرها بواسطة برامج الفدية أو فقدانها أو إتلافها عن طريق الخطأ.

> **بيانات البرنامج** - تعني أي وحدة معلومات تتكون من أحرف أو أرقام أو رموز أو صور أو فيديوهات أو تسجيلات صوتية أو أي مجموعة خليطة منها تتعلق بالمشاركين في البرنامج وتنفيذه ونتائجه. ويشمل هذا البيانات المتاحة في شكل رقمي ومادي.

> سياسة البيانات المسؤولة **الخاصة بمنظمة Mercy Corps** - تهدف سياسة الوكالة إلى وضع مبادئ للاستخدام الشفاف والآمن والمسؤول للبيانات الشخصية على مستوى الوكالة وتطبيق هذه المبادئ في عملنا اليومي.

> **الموافقة المستنيرة** - هي عملية الحصول على الإذن الطوعي لجمع البيانات من أي نوع استنادًا إلى تقدير وفهم واضحين للحقائق والآثار والعواقب المترتبة على أي مشاركة من قِبل المشاركين. ويمكن منح هذه الموافقة إما عن طريق بيان خطي أو شفهي أو عن طريق تصرف دال على الموافقة الواضحة. ويجب الحصول على تلك الموافقة في وقت جمع البيانات الشخصية، أو في أقرب وقت ممكن بشكل معقول بعد ذلك.

> **الموافقة الصريحة** - تتطلب الموافقة الصريحة بيان موافقة واضحًا ومحددًا للغاية. ويجب الاحتفاظ بسجل يوضح متى وكيف تم الحصول على الموافقة وما تم إخبار أصحاب البيانات به بالضبط عند الحصول على موافقتهم. ويجب كذلك في الموافقة الصريحة أن تحدد طبيعة بيانات الفئة الخاصة، كما يجب أن تكون منفصلة عن أي موافقات أخرى تطلبُها.

> **عملية إزالة التعريف** - تعني أي أنشطة أو طرق لمعالجة البيانات من شأنها منع الكشف عن هوية مشارك ما أو شخص آخر بشكل مباشر و/أو غير مباشر. أنواع الأمثلة: إزالة/إخفاء وتجهيل الهوية (أي إزالة كميات معينة من البيانات الشخصية، أو تطبيق مجموعة من القيم على مستوى مجموعات معينة من البيانات الشخصية) واستخدام أسماء مستعارة (أي معالجة البيانات الشخصية بطريقة لا يمكن بها أن تُنسب إلى الأشخاص أو الأُسر أصحاب البيانات المحددين دون استخدام معلومات إضافية مثل المُعرّفات أو تجزئات البيانات الفريدة)

> **معلومات التعريف الشخصية (PII)** – هي المعلومات المتعلقة بشخص طبيعي معين تم تحديده أو يمكن تحديده أو التوصل إلى هويته ("صاحب البيانات")؛ والشخص الذي يمكن التعرّف عليه هو الشخص الذي يمكن تحديد هويته، بشكل مباشر أو غير مباشر، بوجه خاص

عبرالرجوع إلى رقم تعريفي أو لعامل واحد أو أكثر من العوامل الخاصة بهويته الجسدية أو الفسيولوجيّة أو النفسية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية. ترتبط هذه المعلومات ارتباطًا وثيقًا **بمعلومات التعريف الديموغرافية (DII)** التي يمكن استخدامها لتحديد هوية مجتمع أو مجموعة معينة سواء كانت جغرافية أو عرقية أو دينية أو اقتصادية أو سياسية.

> **التخزين الآمن** - يعني أنه يمكن فقط لأعضاء فريق منظمة Mercy Corps الذين لديهم حاجة ضرورية الوصول إلى البيانات مع اتخاذ الخطوات اللازمة لمنع سرقة البيانات وإساءة استخدامها. التخزين الآمن - يعني أنه يمكن فقط لأعضاء فريق منظمة Mercy Corps الذين لديهم حاجة ضرورية الوصول إلى البيانات مع اتخاذ الخطوات اللازمة لمنع سرقة البيانات وإساءة استخدامها. يصبح أي ملف مُخزَّن بشكلٍ آمن عندما:
- يوجد في منصة تستوفي/ تطبق معايير قوية لأمان البيانات وحمايتها وخصوصيتها
- يكون الوصول إليه مقتصرًا على الأطراف المطلوبة فقط
- تتم مراجعة الوصول وتعديله بانتظام حسب الحاجة

> تم وضع متطلبات إضافية لبرامج منظمة Mercy Corps في سياسة المراقبة والتقييم والتعلم الجديدة - ولا سيما المعيار، والتي تقتضي من جميع البرامج ضمان ممارسات التعامل الآمن، وذلك بما يتسق مع سياسة البيانات المسؤولة ومتطلبات الجهات المانحة.

> **أعضاء فريق منظمة Mercy Corps الذين لديهم حاجة ضرورية** - هم أعضاء الفريق الذين يحتاجون إلى الوصول إلى المعلومات المحددة من أجل الوفاء بالمهام المحددة لوظائفهم، مثل تلبية احتياجات المشاركين في البرنامج واستكمال نواتج البرنامج

> **صاحب البيانات** - يعني أي فرد يتم جمع البيانات عنه بشكل مباشر أو غير مباشر أو من خلال طرف خارجي، والذي يمكن تحديد هويته، بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى بياناته الشخصية.

> **حماية البيانات** - تعني حماية معلومات التعريف الشخصية (PII) ومعلومات التعريف الديموغرافية (DII) والبيانات الحساسة الأخرى المتعلقة بأي فرد أو مجموعة ومنع الوصول غير المصرح به إليها أو استخدامها أو توزيعها خلال دورة بيانات إدارة البرنامج أو المشروع أو بعد الانتهاء من البرنامج أو المشروع. تحدد سياسة البيانات المسؤولة الخاصة بمنظمةMercy Corps متطلبات حماية البيانات، كما تخضع الوكالة أيضًا لأطر عمل قانونية/تنظيمية أخرى مثل اللائحة العامة لحماية البيانات (GDPR) الخاصة بالاتحاد الأوروبي.

لمزيد من التعريفات المتعلقة بالبيانات المسؤولة، راجع مستند تعريفات البيانات المسؤولة.

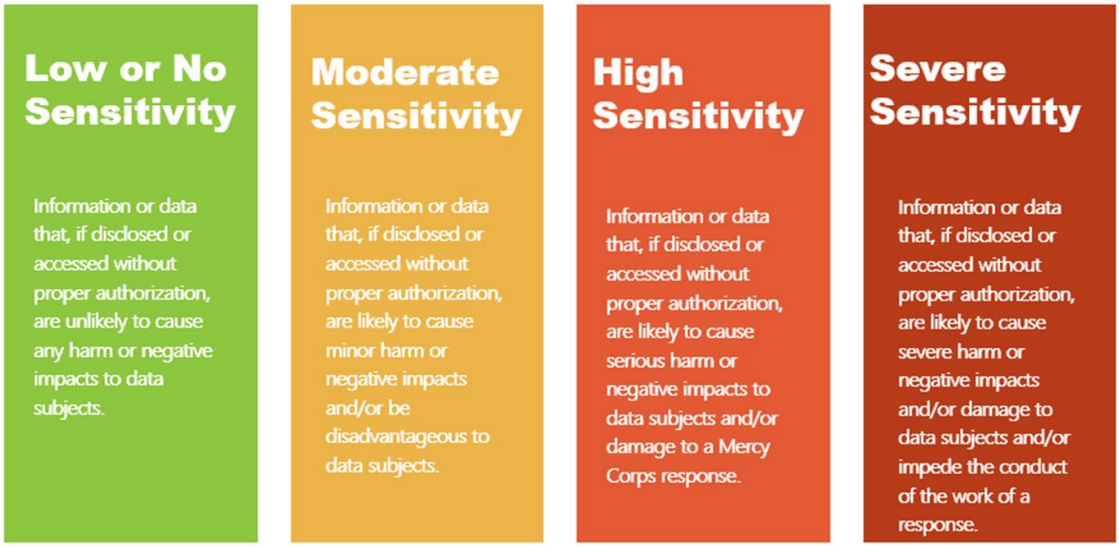
التخطيط

- قم بإيلاء الاعتبار لأنواع البيانات التي سيتم جمعها ووثق ذلك خلال مرحلة التخطيط للمشروع في تقييم تأثير الخصوصية (PIA).
- عندما تتضمن خطة ما جمع و/أو توثيق و/أو تخزين أي نوع من البيانات الحساسة، فيتعين حينئذ إيلاء اعتبار خاص لكيفية استخدام تلك البيانات وسبب استخدامها. وضع في اعتبارك ما إذا كان جمع هذه البيانات ضروريًا لتحقيق النتائج المطلوبة من البرنامج أو المشروع وما إذا كان هناك نوع بيانات بديل سيكون كافيًا لأداء الغرض. يجب جمع البيانات الحساسة فقط إذا كانت ضرورية. يُرجى ملاحظة أن علمية جمع البيانات الحساسة، إذا تم إجراؤها بشكل جيد، تكون عملية مكلفة. ومن خلال رفع عبء جمع البيانات غير الضرورية، فإنك بذلك تسمح للفِرق بتوفير الوقت والموارد للأعمال الأخرى الضرورية. إذا حددت أن معلومات التعريف الشخصية ضرورية، فلا تقم بتطبيق الاختصارات. إذا كانت مواردك المخصصة لجمع البيانات الحساسة وإدارتها غير كافية للقيام بذلك بشكل جيد، فيُرجى إعادة النظر في إجراء تقييم لجميع المخاطر التي قد تسببها للمجتمعات التي تعمل معها.
- قم بإيلاء الاعتبار لأي التقنيات التي سيتم استخدامها لجمع تلك البيانات الحساسة وتخزينها. يجب أن تتضمن التقنيات المستخدمة وسائل حماية مناسبة لجمع المعلومات الحساسة.
- بشكل عام، كلما زادت حساسية البيانات، زادت وسائل الحماية التي تتطلبها. عادةً ما تكون البيانات الحساسة إما "عالية" أو "شديدة" الحساسية (انظر الشكل 1). بالإضافة إلى ذلك، كلما زاد عدد مجموعات البيانات التي يتم جمعها، زادت المخاطر وزادت وسائل الحماية. تتضمن أمثلة وسائل الحماية على سبيل المثال لا الحصر:

- التشفير
- استخدام أسماء مستعارة
- إزالة الارتباط
- تخزين الملفات الورقية في خزائن مقفلة مع تقييد الوصول إليها
- تخزين الملفات على خوادم منظمة Mercy Corps التي تشتمل على مستويات حماية
- قصر الوصول على أجهزة منظمة Mercy Corps وعلى أولئك فقط الذين يجب أن يكون لديهم وصول لتنفيذ مهامهم الوظيفية
- التأكد من قفل الأجهزة، مثل أجهزة الكمبيوتر المحمولة، عندما لا تكون قيد الاستخدام
- بالنسبة للبيانات المكانية، ترتيب نقاط نظام تحديد الموقع العالمي بشكل عشوائي أو تجميعها معًا

- كن واضحًا بشأن الأساس القانوني لمعالجة البيانات الحساسة الذي ستستخدمه وخطط وفقًا لذلك.
- يجب أن تمتثل متطلبات إعداد التقارير في اتفاقيات المِنح بمبادئ "عدم الإضرار" (على سبيل المثال، لا يُطلب من البرنامج جمع المعلومات التي قد تعرض سلامة المشاركين للخطر) ويجب أن تحدد بوضوح الالتزامات والاتفاقيات الخاصة بمنصات مشاركة البيانات والعمليات مع الجهات المانحة والشركاء وأصحاب المصلحة الآخرين، بما في ذلك متطلبات إزالة التعريف وإخفاء وتجهيل الهوية.
- يُعد بروتوكول أمان البيانات على مستوى البرنامج جزءًا من خطة تكنولوجيا المراقبة والتقييم والتعلم (المعيار 6) وهو ما يحدد اعتبارات بيانات أعضاء الفريق بما في ذلك مستويات الأذونات والبروتوكولات الخاصة ببيانات أعضاء فريق منظمة MC وغير أعضاء فريق منظمة MC.
- عندما يتم جمع البيانات الحساسة للأغراض التشغيلية الخاصة بمنظمة Mercy Corps، قم بتخطيط اعتبارات البيانات، بما في ذلك مستويات الأذونات والبروتوكولات، وتحديدها.
- فكِّر في المدة التي تحتاجها للاحتفاظ بالبيانات (فترة الاحتفاظ) وكن قادرًا على تبريرها، وسيعتمد ذلك على أسباب جمعها والمتطلبات القانونية لذلك ومتطلبات الجهات المانحة وسياسات الاحتفاظ بسجلات برامج منظمة MC.
- قم بتبني عملية لتدمير البيانات عند استيفاء فترات الاحتفاظ.

الشكل 1:



التخطيط لجمع البيانات

- إتمام تقييم تأثير الخصوصية من أجل كلٍ من تحديد وإدارة مخاطر خصوصية البيانات المرتبطة بأي نشاط جديد، مثل البرامج الجديدة أو التكنولوجيا الجديدة أو المورّدين الجدد. وعندما يتم جمع البيانات الحساسة، يجب مراجعة تقييم تأثير الخصوصية ذلك من قِبل فرد مختص. سيكون هذا الفرد إما فريق حماية البيانات والخصوصية، أو مسؤول حماية البيانات لديك، أو ما تحدده سياسة المراقبة والتقييم والتعلم، (الحد الأدنى للمعيار رقم 9 - خصوصية البيانات وأمانها):
  - الرئيس القُطري المسؤول، أو رئيس البرامج، أو مدير البرنامج أو رئيس المجموعة
  - مسؤول إدارة المعرفة/المراقبة والتقييم والتعلم بالبرنامج الموصى به والمعني

- قم بإتمام تقييم المعلومات الحساسة (SIA) المتعلق بتقييم تأثير الخصوصية. ويجب أن يوثق هذا التقييم كافة وسائل الحماية الإضافية التي يتم استخدامها في حماية البيانات الحساسة.

- إذا كانت الموافقة هي الأساس القانوني الذي يتم الاستناد إليه، فسوف تتطلب الموافقة المستنيرة حينئذ إبلاغ الأشخاص الذين هم أصحاب البيانات بما يلي بلغة واضحة:
  - أي البيانات التي يتم جمعها ولماذا يُطلب جمعها
  - من الذي ستتم مشاركتها معه بما في ذلك أي شركاء خارجيين وجهات مانحة
  - ما إذا كان سيتم مشاركة البيانات ستتم دوليًا
  - ما طول المدة التي سيتم الاحتفاظ بالبيانات خلالها

- يجب الاحتفاظ بسجل يوضح متى وكيف تم الحصول على الموافقة وما تم إخبار أصحاب البيانات به. يجب تضمين نموذج يشتمل على ما سيُقال إلى أصحاب البيانات للحصول على موافقتهم في مرحلة التخطيط.

جمع البيانات

- يتم تطبيق بروتوكول جمع البيانات على كل حالة من حالات جمع البيانات والذي يشمل ما يلي:
    - وسائل الحماية الإضافية للبيانات الحساسة
    - التعليمات الموثقة لجمع البيانات وتنظيفها ومراجعتها وإزالة التعريف فيها، حسب الاقتضاء.
    - الإرشادات بشأن انتهاكات أمن البيانات المحتملة لجميع البيانات الكمية والنوعية التي تم جمعها (على سبيل المثال، الأجهزة المفقودة أو المسروقة، وعمليات تسجيل الدخول المُخترَقة، وما إلى ذلك)
    - تعليمات استخدام النماذج الورقية وحمايتها أثناء جمع البيانات
    - إجراء عمليات التحقق الفورية ومراقبة مدى التزام الشخص/الأشخاص ببروتوكولات الحماية والتأمين عند جمعهم للبيانات
- يجب ربط جميع ما سبق بتقييم المعلومات الحساسة

تخزين البيانات

- يجب أن يقتصر الوصول إلى الملفات التي تحتوي على معلومات حساسة على أعضاء الفريق الذين يحتاجون إلى الوصول إليها لتحقيق النواتج الضرورية، كما يجب أن يتم إجراء تجهيل هوية منهجي للمعلومات الحساسة قبل ربطها بنظام TolaData أو مشاركتها مع أي طرف خارجي حسب الاقتضاء. يوفر المعيار 8 من سياسة المراقبة والتقييم والتعلم 8 إرشادات إضافية بشأن أفضل ممارسات حفظ وتخزين بيانات المراقبة والتقييم والتعلم
- يتم تخزين البيانات في موقع ممتثل لجميع سياسات منظمة Mercy Corps ذات الصلة (على سبيل المثال، "سياسة البيانات المسؤولة"، و"الاستخدام المقبول").
- يُحظر الاحتفاظ بالبيانات الحساسة لمدة تزيد عن الوقت الضروري. عند استيفاء فترات الاحتفاظ، يجب تدمير البيانات بشكل آمن أو تجهيل هويتها بالكامل.
- يجب توثيق فترات الاحتفاظ وتبريرها.
- تذكر- يمكن أيضًا تخزين البيانات في أنظمة جمع البيانات المتنقلة. تنطبق جميع اعتبارات تخزين البيانات المذكورة أعلاه على أنظمة جمع البيانات المتنقلة أيضًا.

تحليل البيانات

- يوجد بروتوكول لمشاركة البيانات مع الاستشاريين وفرق المقر الرئيسي والشركاء وأصحاب المصلحة، بما في ذلك على سبيل المثال لا الحصر اتفاقيات مشاركة البيانات، والموافقات من قبل فريق المراقبة والتقييم والتعلم القُطري، والأدوار والمسؤوليات وما إلى ذلك.
- يتم توقيع اتفاقيات عدم الإفصاح (NDA) من قِبل جميع الاستشاريين قبل وصولهم إلى أي مجموعات بيانات مملوكة لمنظمة Mercy Corps.

تقديم البيانات إلى جهة مانحة أو شريك أو طرف خارجي آخر (إذا كان ذلك مناسبًا)

- يتم تجهيل هوية البيانات الخام ومراجعتها للتأكد من امتثالها لمبادئ "عدم الإضرار" قبل تقديمها.
- يُحظر مشاركة البيانات الحساسة مع أي طرف خارجي لم يتم ذكره كجزء من عملية الموافقة المستنيرة.
- يُحظر مشاركة البيانات الحساسة مع أي طرف خارجي ما لم تكن هناك اتفاقية مشاركة بيانات مُبرمة معه.
- استخدم فقط الأنظمة التنظيمية المُصرح بها لمشاركة المستندات، مثل Google Drive أو Microsoft Sharepoint، وليس منصات المشاركة الخاصة بطرف خارجي.

الأسئلة الشائعة

لضمان امتثالنا لمتطلبات التنوع، نطلب من أعضاء الفريق الإشارة إلى حالتهم العِرقية في نماذج طلب الوظيفة - هل يتعين عليّ القيام بأي شيء حيال ذلك الأمر؟

نعم، تُعتبر البيانات المتعلقة بالأصل العِرقي أو الإثني بيانات شخصية حساسة، لذا ستحتاج إلى اتباع إرشادات البيانات الحساسة وتطبيق وسائل الحماية الإضافية على تلك البيانات.

ماذا يحدث إذا قمت أنا أو أحد أعضاء الفريق بمشاركة بيانات حساسة عن غير قصد؟ ما هي الإجراءات العلاجية التي يمكن اتخاذها؟

عند اكتشاف المشاركة العرضية للبيانات الشخصية، يجب أن يتم وقف مشاركة تلك البيانات على الفور. قد يعني هذا مطالبة المستلم العرضي بحذف أي نسخ من البيانات، أو إلغاء وصول المستلم العرضي إلى البيانات، أو جعل البيانات في وضع عدم الاتصال بالإنترنت، أو اتخاذ خطوات أخرى حسب الحاجة.

تُشكِّل المشاركة العرضية أو غير المقصودة للبيانات الشخصية انتهاكًا للبيانات ويجب عليك إخطار **it-security@mercycorps.org** على الفور وفقًا لخطة الاستجابة للحوادث. ويجب تقديم أكبر قدر ممكن من المعلومات، في أقرب وقت ممكن، حول طبيعة البيانات التي تمت مشاركتها.

ما الذي يتعين عليّ القيام به عندما أرى أحد أعضاء الفريق يتعمد مشاركة بيانات حساسة مع شخص لا ينبغي أن يكون لديه حق الوصول إلى تلك البيانات؟

تُعد مشاركة البيانات الحساسة عمدًا مع شخص غير مصرح له الوصول إليها أمرًا بالغ الخطورة حيث يمكن أن يؤدي إلى إلحاق ضرر جسيم بصاحب البيانات والوكالة. إذا رأيت أحد أعضاء الفريق يتعمد مشاركة معلومات حساسة بهذه الطريقة، فيجب عليك حينئذ إبلاغ مدير البرنامج أو المدير الإقليمي أو مديرك بهذا الأمر على الفور.

تُعد مشاركة البيانات الحساسة مع أولئك الذين يُحظر وصولهم إليها انتهاكًا للبيانات، ويجب الإبلاغ عن هذا الأمر إلى it-security@mercycorps.org على الفور وفقًا لخطة الاستجابة للحوادث. ويجب تقديم أكبر قدر ممكن من المعلومات، في أقرب وقت ممكن، حول طبيعة البيانات التي تمت مشاركتها.

كيف يقرر البرنامج من الذي يجب/لا يجب أن يكون لديه حق الوصول إلى البيانات الحساسة؟

يجب منح الوصول إلى البيانات الحساسة فقط إلى الأفراد الذين يحتاجون إلى الوصول من أجل القيام بدورهم. يجب إخفاء هوية البيانات الحساسة دائمًا قبل مشاركتها، إذا أمكن. تشمل الأمثلة الشائعة لإخفاء الهوية كلاً من إخفاء وتجهيل الهوية أو استخدام أسماء مستعارة.

ما هي البيانات مُزالة الارتباط؟

تعني البيانات مُزالة الارتباط البيانات التي تمت إزلة ارتباطها تمامًا وبشكل نهائي بصاحب البيانات بحيث لم يعد من الممكن إعادة ربط تلك البيانات بصاحب البيانات. وتُعد البيانات مُزالة الارتباط نوعًا من البيانات مُجهَّلة الهوية.

هل يجب أن أقوم بتمكين التنبيهات بشأن الوصول إلى مجموعة البيانات الإلكترونية من قِبل أي شخص غير مصرح له الوصول إليها؟

إذا كان من الممكن تشغيل تنبيهات الوصول غير المصرح به، فيجب تمكينها دائمًا حينئذ؛ ومع ذلك، لا تتوفر هذه الإمكانية في جميع المنصات الإلكترونية. تحقق من إعدادات النظام في منصتك، وقم بتمكين التنبيهات إذا كان ذلك ممكنًا.

هل ينبغي على أعضاء الفريق استخدام أجهزتهم الشخصية لجمع المعلومات الحساسة أو تخزينها؟ إذا كان الأمر كذلك، فما هي أشكال الحماية التي ينبغي توفيرها؟

يُحظر استخدام الأجهزة الشخصية لجمع المعلومات الشخصية أو تخزينها، بما في ذلك معلومات المشاركين، *ما لم يتم تثبيت برنامج إدارة الجهاز المناسب* وتضمين استخدام الأجهزة الشخصية في تقييم تأثير الخصوصية الخاص بالمشروع. ويُحظر أيضًا استخدام الأجهزة الشخصية مطلقًا لجمع بيانات المشاركين دون الحصول على موافقة مسؤول البرنامج الصريحة. كما يُحظر استخدام الأجهزة الشخصية لجمع أو تخزين المعلومات الحساسة.

هل يمكن للجهة المانحة الخاصة بي أن تدقق في كيفية تعاملي مع البيانات الحساسة؟

نعم، تطلب العديد من الجهات المانحة إجراء تدقيقات داخلية وتقوم أيضًا بإجراء تدقيقات وتقييمات خارجية لجودة البيانات. تتمثل إحدى جوانب هذه التقييمات في تقييم قدرة نظام المراقبة والتقييم والتعلم على مواجهة الصدمات والاختراقات وتهديدات الأمان، خاصة إذا كان البرنامج يجمع معلومات حساسة.

هل أقوم بربط قوائم المشاركين بنظام **TolaData** كدليل؟

يمكن ربط قوائم المشاركين (على سبيل المثال، قوائم حضور التدريب، وما إلى ذلك) كدليل نظرًا لأنه يجب وضع هذا الدليل وتخزينه خارج نظام TolaData، وبالتالي لن يتمكن سوى أشخاص معينين من الوصول إلى هذا الدليل استنادًا إلى أذونات مِرفق التخزين الخارجي ذلك. ويتعين النظر في ما إذا كان أي نوع من الأدلة المرتبطة بنظام TolaData يتطلب إدراج المعلومات الشخصية. ويُعد من المستبعد جدًا أن يكون إدراج المعلومات الحساسة ضروريًا.

كيف أعرف ما إذا كان موردو أو منصات تكنولوجيا جمع البيانات أو تخزينها ممتثلة لمتطلبات البيانات الحساسة؟

تمتثل بالفعل منصات جمع البيانات وتخزينها الحالية المتضمنة في مجموعة تكنولوجيا المراقبة والتقييم والتعلم مع متطلبات البيانات الحساسة، وذلك شريطة أن يكون قد تم تكوينها بشكل مناسب لاستخدام وسائل الحماية والبروتوكولات المذكورة في هذه الوثيقة. وفي حال كان سيتم استخدام منصة من خارج مجموعة تكنولوجيا المراقبة والتقييم والتعلم، فيجب حينئذ إتمام تقييم تأثير الخصوصية (PIA) لتقييم ما إذا كان يمكن اعتبار تلك المنصة ممتثلة لمتطلبات البيانات الحساسة من عدمه. فيما يتعلق بتقييم مورّد تكنولوجيا ما واستعداده للامتثال لسياسة البيانات المسؤولة ومتطلبات البيانات الحساسة، يكون تقييم تأثير الخصوصية أيضًا أفضل أداة لتحديد ما إذا كانت ممارساته ستصبح ممتثلة من عدمه.

كيف يمكنني معرفة ما إذا كانت البيانات تُعد بيانات شخصية أم حساسة؟

إذا كنت تقوم بمعالجة البيانات التي تندرج تحت أي فئة من فئات البيانات الحساسة من فئة خاصة الموضحة في اللائحة العامة لحماية البيانات (انظر **البيانات الحساسة من فئة خاصة** أعلاه)، فستكون هذه البيانات دائمًا بيانات حساسة. إذا كان هناك سبب خاص بالسياق يجعل البيانات تندرج تحت فئة "الحساسية الشديدة" (انظر الشكل 1 أعلاه)، فيجب حينئذ أيضًا تصنيف تلك البيانات على أنها بيانات حساسة.

الوثائق ذات الصلة:

الموافقة

أداة المراقبة والتقييم والتعلم: نموذج الموافقة المستنيرة (للمشاركين في المقابلات الشخصية)

إرشادات الموافقة المستنيرة بشأن مشاركة بيانات آليات إبلاغ المساءلة المجتمعية

إرشادات المراقبة والتقييم والتعلم عن بُعد فيما يتعلق بجائحة كوفيد-19

التشفير

استخدام Ona.io في منظمة Mercy Corps: نماذج التشفير والبيانات الحساسة

البيانات البيومترية

البيانات البيومترية لدى منظمة Mercy Corps:الأساس الداخلي

الأدلة العامة

- مجموعة أدوات مسؤولية البيانات - دليل للممارسين المستخدمين للنقد والقسائم - https://www.calpnetwork.org/wp-content/uploads/2021/03/Data-Responsibility-Toolkit_A-guide-for-Cash-and-Voucher-Practitioners.pdf
- مجموعة أدوات ELAN Data Starter Kit للموظفين الميدانيين العاملين في المجال الإنساني: v_ https://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf
- دليل اللجنة الدولية للصليب الأحمر بشأن حماية البيانات في العمل الإنساني: https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

تجهيل هوية المعلومات

إرشادات وزارة الزراعة الأمريكية بشأن مراجعة معلومات التعريف الشخصية (PII) في تقييمات المشروعات

معمل مكافحة الفقر "إزالة التعريف لنشر البيانات"

إنشاء رموز فريدة للمشاركين في البرنامج أو أصحاب البيانات الآخرين

مشروع الإرشادات من فريق التكنولوجيا من أجل التنمية (T4D)

التقييمات

تقييم تأثير الخصوصية (PIA) - القالب

تقييم تأثير الخصوصية (PIA) - الإرشادات

تقييم المعلومات الحساسة (SIA)