

استخدام دورة حياة البيانات لإدارة البيانات المختصة



OXFAM

ما هي إدارة البيانات المختصة؟

سوف تساعد هذه النشرة أي شخص على التعامل مع بيانات البرنامج أو مشاركتها أو الوصول إليها بشكل صحيح للنظر في قضايا البيانات المختصة طوال **دورة حياة البيانات**.

وهو يركز أساسا على إدارة البيانات المختصة في الأزمات الإنسانية من منظور جمع البيانات. ومع ذلك، تنطبق المبادئ والأدوات والنهج أيضا على نطاق واسع.

تعتمد إدارة البيانات المختصة على معالجة البيانات التي نقوم بجمعها باحترام، والتمسك بحقوق المجيبين- وهم الأشخاص الذين نقوم بجمع بياناتهم. وتتضمن البيانات: استجابات المسح، معلومات التسجيل، والصور، والقصص، إلخ.

لا يجب أن تكون إدارة البيانات المختصة مقيدة. وعلى العكس من ذلك، يمكن أن تعزز وتيسر مساهمة البيانات في الاعمال عالية الجودة. ينبغي أن ينظر إليها كإطار لضمان استجابة جامعي البيانات والتزامهم بالمساءلة وإيصال الأصوات.

يتغير الإطار التنظيمي لإدارة البيانات (القوانين والمعايير الأخرى) بسرعة، وكذلك تكنولوجيات جمع وإدارة البيانات. إذن تعتبر إدارة البيانات المختصة عملية تتطور باستمرار حول تحديد متى وكيفية جمع البيانات، وكيفية إدارة المخاطر.



1 وضع خطة

حدد بوضوح الغرض من جمع البيانات.

ينبغي أن تكون الفوائد التي تتوقعها من البيانات متناسبة مع المخاطر. وينبغي أن تحكم بمصالح وحياة السكان المتضررين.

قم بتقييم الأساليب والأدوات المتاحة للعثور على أولئك الأكثر ملاءمة للسياق ولغرضك.

قلل من الأسئلة، وتحقق بدقة إذا كنت حقاً بحاجة أن تسأل. تحقق أيضاً من أنه لم يتم جمع المعلومات من قبل من مصدر موثوق به.

هل تحتاج إلى القيام بإجراء حماية المعلومات / **تقييم لأثر خصوصية البيانات**؟

تعتبر **البيانات الشخصية** حساسة للغاية وتحتاج إلى حماية إضافية، مثل التخزين بشكل منفصل عن إجابات المستجيبين، أو اتخاذ تدابير **لحفظ** البيانات.

يجب وجود خطة من البداية تكفل الحصول على **موافقة مدروسة**. وأن توضح ما هي الموافقة، بالإضافة إلى توعية المجتمعات عن غرض البيانات التي تجمعها.

تحقق من إمكانية وجود خطر التحيز في عملية الاستهداف والمنهجية. كيف سيتم التحقق من دقة بياناتك؟



2 القيام بتقييم المخاطر

من الممكن أن يعرض جمع البيانات الأشخاص للخطر. لذلك قم بتقييم المخاطر واتخاذ إجراءات لتجنب العواقب السلبية للمجيبين، مثلًا ضمان أمن البيانات وسريتها.

استخدم خبراء تقنيين لفهم مخاطر محددة، وفكر من خلال ما تفعله في إمكانية حدوث **خرق للبيانات** أو مشكلة ما.



3 تدريب العدادين

عند تدريب جامعي البيانات:

- قم بتغطية اعتبارات البيانات المختصة.
- قم بتغطية عملية الموافقة. ماذا ينبغي أن أعرف المجيبين حول ما سوف يحدث لبياناتهم الخاصة؟
- استخدم سيناريوهات حقيقية لتقديم التدريب على نظم وبروتوكولات في الحياة.



4 الحصول على الموافقة المدروسة

لا تعتبر الموافقة مجرد عملية تعبئة مربع في جدول - بل هي عبارة عن معاملة المجيبين باحترام والحفاظ على كرامتهم، فضلا عن التمسك بالشروط القانونية المتعلقة بالبيانات الشخصية.

أخبر المجيبين كيف سيتم استخدام بياناتهم الخاصة، ولماذا تحتاجها، كيفية تخزينها، مع من سيتم مشاركتها، كيفية ضمان أن هذه المجموعات لن تقوم بمشاركتها، وكيف يمكنهم الاتصال بك في حال تم تغيير رأيهم بخصوص الموافقة.

اسأل المجيبين إذا كانوا يريدون الحصول على تغذية راجعة بشأن ما يمكنك القيام به بمعلوماتهم الخاصة.

أعطِ المجيبين فرصة للتعطيل، وضع خطة بديلة في حال حصل ذلك.

5 إدارة البيانات



كن حذرا عند استخدام الأجهزة المحمولة وتبادل التكنولوجيا. **استخدم التشفير** عند الضرورة وقم بإعداد الأنظمة التي تسمح للهواتف بمحو البيانات عن بعد.

اتخذ مزيدًا من الحذر عند التعامل مع العمليات الورقية وعند نقل نسخ مطبوعة في الميدان. استخدم تشفير الملفات الرقمية عند نقطة إدخال البيانات.

الدخول

قم بإعداد حسابات فردية باستخدام كلمات مرور للمستخدم للدخول إلى مصادر البيانات الرقمية، أعطِ الأولوية للذين بحاجة إلى الوصول إلى شيء ما.

يكون كل شخص يقوم بجمع أو استخدام البيانات مسؤولاً عن إدارة البيانات المختصة. استخدم نهج إعطاء مسؤولية حماية البيانات لعضو واحد من الفريق، مع ضمان تفهم الجميع لأدوارهم ومسئولتهم.

التخزين

افحص بعناية أمن البيانات والموقع من خيارات قاعدة البيانات والتخزين.

لعملية جمع الأوراق، فكر في خيارات التخزين الآمن. قم بتخزينها في خزنة آمنة أو مؤمنة إذا كان ذلك ممكناً

المشاركة

قم بإعداد **اتفاق تبادل البيانات** مع المنظمات التي يمكنك مشاركة البيانات معها، بما في ذلك إرشادات معالجة البيانات.

التمس المشورة القانونية إذا لزم الأمر.

تنطبق هذه المبادئ على الجميع بغض النظر عن ماهية الطرف الثالث: الحكومة، منظمة غير حكومية أخرى، شركة خاصة، البنك، إلخ.

لا تشارك البيانات دون الحصول على موافقة من المجيبين.

تنشر بعض المنظمات البيانات. التمس المشورة المتخصصة وقم بفحص المخاطر والحساسيات قبل نشر **أي مجموعة من البيانات**. لا يكفي ببساطة إزالة الأسماء لإخفاء الهويات.



6 استخدم البيانات للقيام بشيء ما

قد يكون ذلك للضغط، والدعوة، أو إدخال تعديلات على البرامج.

فكر فيما تمثله البيانات.
هل راعيت التوازن بين الجنسين؟

هل هناك أي تحيز في القرار مبني على أساس البيانات؟



7 الملكية والتغذية الراجعة

كيف يمكنك تعزيز الملكية من المجيبين؟

اجتمع مع المجيبين للتحقق من صحة النتائج والتأكد من أنها تمثل وجهات نظرهم حيثما كان ذلك ممكناً. قدم لهم التغذية الراجعة بشأن ما حدث مع بياناتهم الخاصة.



8 الاحتفاظ/التخلص

خطط دائماً للمدة التي تحتاجها للاحتفاظ بالبيانات - تذكر بأن البيانات تفقد أهميتها بسرعة كبيرة.

لا يعد حذف مستندات رقمية كحرق أو تمزيق ملف مادية، لأنه كثير ما يكون قد تم ترك السجلات الرقمية على جهاز الكمبيوتر الخاص بك (مثل تنزيل المجلدات، والمحفوفات، إلخ. هذا هو المعروف بالبيانات المؤجلة).

معجم الكلمات

التشغير هو تحويل البيانات إلى رموز لا يسهل فهمها من قبل أشخاص غير مصرح لهم بذلك.

الموافقة المدروسة هي اتفاق يتم بطوعية وبحرية، يستند إلى تقديرات واضحة وفهم للحقائق

والآثار والعواقب المستقبلية للعمل. يجب أن يكون الأفراد على علم بحقهم في رفض الموافقة وقدرتهم على ممارسة ذلك الحق. وهناك بعض الحالات التي لا يمكن فيها الموافقة، على سبيل المثال مع الأطفال، أو الأشخاص ذوي الإعاقة.

البيانات الشخصية هي المعلومات التي يمكن استخدامها، بمفردها أو مع معلومات أخرى، لتحديد الشخص.

تقييم أثر الخصوصية هي أداة لتحديد وتقليل مخاطر الخصوصية.

إخفاء الهوية: نظرياً، يعني هذا أنه من الصعب أو المستحيل تحديد هوية شخص عن طريق مجموعة بيانات. في الواقع، يمكن غالباً تجميع مجموعة من البيانات للكشف عن الهويات.

الإخلال بالبيانات هو الإفصاح عن المعلومات الذي من الممكن أن يكون مقصوداً أو غير مقصود، إلى بيئة غير موثوق بها.

دورة حياة البيانات هي تدفق المعلومات من خلال نظام، ابتداءً من الإنشاء والتخزين إلى الحذف.

مجموعة البيانات هي عبارة عن مجموعة من البيانات ذات الصلة.

اتفاق تبادل البيانات هو إطار لتقاسم البيانات التي تحدد كيفية إرسال البيانات، وتخزينها واستخدامها.

لمزيد من المعلومات

www.oxfam.org.uk/responsibledata

دورة حياة البيانات المختصة

