OCHA centre for humdata

مركز البيانات الإنسانية

سلسلة المذكرات الإرشادية

مسؤولية البيانات في العمل الإنساني

النهج المسؤولة لمشاركة البيانات

النقاط الرئيسية:

- المشاركة المفتوحة للبيانات الدقيقة وفي الوقت المناسب أمر ضروري للاستجابة الإنسانية الفعالة والكفؤة. تتعلق كيفية تعامل المنظمات الإنسانية مع مشاركة البيانات بالثقة والتعاون في القطاع.
- مع نمو نظام بيانات العمل الإنساني، تصبح الفرص والمخاطر لمشاركة البيانات أوضح، مما يدفع المنظمات إلى استكشاف نهج أكثر تحديدًا لمشاركة البيانات.
- تعترف المنظمات الإنسانية على نطاق واسع بحساسية البيانات الشخصية: فتعرضها ينطوي على احتمال كبير للتسبب في ضرر. الغالبية العظمى من البيانات غير الشخصية آمنة للمشاركة المفتوحة، ولكن يمكن أن تكون البيانات غير الشخصية أيضًا حساسة ويجب التعامل معها بحذر.
- يجب على المنظمات الإنسانية أن تأخذ في الاعتبار أربعة عوامل عند اتخاذ قرار مشاركة البيانات غير الشخصية: (i) الفائدة؛ (ii) الحساسية؛ (iii) القدرة البشرية والتقنية؛ و(iv) الحوكمة.
- يجب على المنظمات الإنسانية تحديد ومقارنة جميع النهج المتاحة لمشاركة البيانات، مع مراعاة النهج الأكثر انفتاحًا أولاً والعمل على النهج الأكثر تحديدًا حسب الضرورة.

المقدمة

أصبح استخدام وتبادل البيانات من الوظائف الأساسية للمنظمات الإنسانية. يحتاج الموظفون بانتظام إلى اتخاذ قرارات بشأن ما إذا كان ينبغي وكيفية مشاركة بيانات منظماتهم، حتى إذا لم يكن دورهم يركز أساسًا على إدارة البيانات أو المعلومات. بالإضافة إلى ذلك، نما الاهتمام بمشاركة واستخدام البيانات التي يتم إنتاجها في العمل الإنساني. استجابةً لهذا الاهتمام، شهد القطاع الإنساني زيادة كبيرة في إنتاج البيانات ومشاركتها في السنوات الأخيرة.

> "البيانات الدقيقة هي شريان الحياة لصنع السياسات واتخاذ القرارات الجيدة. الحصول عليها ومشاركتها عبر مئات المنظمات في وسط الطوارئ الإنسانية أمر معقد ويستغرق وقتًا،لكنه بالغ الأهمية."
>
> - الأمين العام للأمم المتحدة أنطونيو غوتيريش في افتتاح مركز البيانات الإنسانية في لاهاي في ديسمبر ٢٠١٧.

المشاركة المفتوحة للبيانات الدقيقة وفي الوقت المناسب أمر ضروري للاستجابة الإنسانية الفعالة والكفؤة ويجب أن تظل هدفًا رئيسيًا للقطاع. على سبيل المثال، البيانات الوبائية لـ COVID-١٩[١] التي جمعتها وشاركتها يوميًا مركز جامعة جونز هوبكنز لعلوم النظم والهندسة تم دمجها في عدد من لوحات التحكم وتقارير الوضع لصناع القرار في جميع أنحاء القطاع الإنساني منذ بداية الجائحة. بحلول ديسمبر ٢٠٢٠ تم تنزيل هذه المجموعة من البيانات أكثر من ٣٢٠،٠٠٠ مرة من تبادل البيانات الإنسانية (HDX) منذ نشرها لأول مرة على المنصة في يناير من ذلك العام. يتم تعزيز فائدة البيانات المفتوحة للممارسين الإنسانيين بشكل أكبر من خلال حقيقة أن استخدام HDX في البلدان التي لديها خطة استجابة إنسانية (HRP) قد نما بشكل أسرع بكثير من الاستخدام في المواقع الأخرى.[٢]

طريقة تعامل المنظمات الإنسانية مع مشاركة البيانات تتعلق مباشرة بالثقة والتعاون في القطاع. إن الحفاظ على الثقة داخل نظام البيانات هو أمر حاسم لاستدامة مشاركة البيانات ويتعلق بقضايا مثل جودة البيانات، والدرجة التي سيتم تأمين البيانات بها بعد المشاركة والاستخدام المسؤول للبيانات من قبل المستلم. لأن البيانات في القطاع الإنساني غالبًا ما تتعلق بالفئات الأكثر عرضة للخطر، فإن إدارة ومشاركتها تتطلب الحذر.

طورت العديد من المنظمات الإنسانية أو حدّثت إرشاداتها وحوكمتها وممارساتها لدعم جوانب مختلفة من مسؤولية البيانات: الإدارة الآمنة والأخلاقية والفعالة للبيانات. كما شهد القطاع زيادة في عدد الجهود التعاونية لتحسين مسؤولية البيانات خارج المنظمات الفردية.[٣] ومع ذلك، بينما يتعلم النظام الإنساني المزيد عن المخاطر المرتبطة بمشاركة البيانات، تواجه المنظمات تحديات أكثر تعقيدًا في مشاركة هذه البيانات بمسؤولية.[٤]

تهدف هذه المذكرة الإرشادية إلى دعم اتخاذ القرارات حول مشاركة البيانات غير الشخصية في البيئات الإنسانية. تشرح حساسية البيانات، وتوفر أمثلة شائعة للبيانات غير الشخصية الحساسة، وتوضح نهجًا لتصنيف حساسية المعلومات والبيانات في البيئات الإنسانية. كما تقدم إطارًا يمكن للمنظمات استخدامه لوزن أربعة عوامل تساعد في تحديد ما إذا كان يمكن مشاركة البيانات وتشرح النهج الشائعة للقيام بذلك بمسؤولية.

خيارات مشاركة البيانات على تبادل البيانات الإنسانية (HDX)

عندما تم إطلاق تبادل البيانات الإنسانية (HDX) في عام ٢٠١٤، كان يحتوي على حوالي ٩٠٠ مجموعة بيانات، تم مشاركتها من قبل عدد قليل من المنظمات "المتبنية المبكرة". بحلول نهاية عام ٢٠٢٠، نما هذا العدد ليصل إلى أكثر من ١٨،٠٠٠ مجموعة بيانات. فقط المنظمات المعتمدة يمكنها مشاركة البيانات على المنصة. يمكنهم جعل البيانات متاحة للجمهور لأي شخص يزور الموقع أو بشكل خاص لأعضاء منظماتهم فقط.

في عام ٢٠١٧، أضاف فريق HDX خيارًا آخر لمشاركة البيانات: HDX Connect. تتيح هذه الميزة للمنظمات نشر البيانات الوصفية فقط، مع إتاحة البيانات الأساسية عند الطلب. إذا تم منح الوصول، يتم مشاركة البيانات بشكل ثنائي دون المرور عبر منصة HDX. على سبيل المثال، تستخدم منظمة Ground Truth Solutions HDX Connect لتوفير الوصول إلى بيانات تصورات المجتمع حول COVID-١٩ التي تم جمعها في العراق.

كجزء من عملية ضمان الجودة، يقوم فريق HDX أيضًا بإجراء تقييم لمخاطر الإفصاح على أي مورد يضاف إلى المنصة يحتوي على بيانات دقيقة. يقوم فريق HDX بذلك لأنه قد يكون من الممكن إعادة تحديد الأفراد أو كشف المعلومات السرية حتى بعد إزالة المعرفات المباشرة من البيانات الدقيقة.

أصبحت بعض المنظمات على HDX أكثر توجهًا نحو الوصول المراقب إلى بياناتها، إما بسبب الطبيعة الحساسة للبيانات، أو زيادة الضغط لتتبع كيفية استخدام البيانات والإبلاغ عنها، أو القيود المتعلقة بالموارد واستدامة العمليات. سيظل HDX دائمًا يدعم طرقًا مختلفة لمشاركة البيانات - ومع ذلك، يظل الوصول المفتوح هو الخيار الأفضل لغالبية البيانات التي يتم إنتاجها للاستجابة الإنسانية.

[١] بالوصول إلى بيانات حالات فيروس كورونا المستجد (COVID-١٩) على منصة HDX.

[٢] "من أغسطس ٢٠١٦ حتى أغسطس ٢٠٢٠ (الفترة التي تتوفر فيها البيانات)، كان النمو في عدد المستخدمين الشهريين من الدول التي لديها خطة استجابة إنسانية (HRP+) بنسبة ٩٤٣٪ مقارنة بـ ٥٦٦٪ في جميع الدول." من دراسة حالة HDX، سبتمبر ٢٠٢٠.

[٣] تشمل هذه، على سبيل المثال، مجموعة العمل الفرعية التابعة للجنة الدائمة المشتركة بين الوكالات (IASC) بشأن مسؤولية البيانات في العمل الإنساني، ومبادرة إدارة معلومات الحماية، ومبادرة البيانات المسؤولة للأطفال، من بين أمور أخرى.

[٤] لفهم أفضل للتحدي الذي تواجهه المنظمات الإنسانية عند مشاركة البيانات تحديدًا في الأزمات الإنسانية المطولة، انظر ALNAP، جمع البيانات وتحليلها واستخدامها في الأزمات الإنسانية المطولة، يونيو ٢٠٢٠.

فهم حساسية البيانات

تعترف المنظمات الإنسانية على نطاق واسع بحساسية البيانات الشخصية: فتعرضها ينطوي على احتمال كبير للتسبب في ضرر. لا يزال هذا الفهم غير موجود على نطاق واسع بالنسبة للبيانات غير الشخصية، التي تغطي عادة الفئات الثلاث التالية في البيئات الإنسانية[٥]:

١. البيانات حول السياق الذي تجري فيه الاستجابة (مثل الأطر القانونية، الظروف السياسية والاجتماعية والاقتصادية، البنية التحتية، إلخ) والوضع الإنساني (مثل الحوادث الأمنية، مخاطر الحماية، المحركات للوضع أو الأزمة).

٢. البيانات حول الأشخاص المتأثرين بالوضع واحتياجاتهم، والتهديدات ونقاط الضعف التي يواجهونها، وقدراتهم.

٣. البيانات حول الجهات الفاعلة في الاستجابة الإنسانية وأنشطتها (مثل ما هو مذكور في 3W/4W/5W).

الغالبية العظمى من هذه البيانات آمنة للمشاركة بشكل مفتوح. ومع ذلك، يمكن أن تكون البيانات غير الشخصية حساسة أيضًا. تشمل أمثلة البيانات غير الشخصية الحساسة البيانات حول المجموعات التي تتعرض للعنف القائم على النوع الاجتماعي أو موقع الأقليات العرقية في مناطق النزاع. تُعتبر هذه البيانات حساسة لأنها تُمكن من تحديد مجموعات الأفراد بواسطة عوامل تحديد ديموغرافية، مثل العرق، الجنس، العمر، المهنة، الدين أو موقع الأصل. يمكن أيضًا أن تخلق البيانات غير الشخصية مخاطر بطرق أخرى، على سبيل المثال عن طريق كشف مواقع المرافق الطبية في المناطق التي تكون عرضة للهجوم. مع استمرار نمو الوعي بالمخاطر المرتبطة بمشاركة هذه البيانات، تتحول بعض المنظمات من التركيز على البيانات المفتوحة إلى المشاركة الأكثر تحكمًا.

لدى العديد من المنظمات تصنيفات لحساسية المعلومات والبيانات (انظر الشكل ١ أدناه) التي تحدد أي البيانات تقع في أي فئة من الحساسية لتسهيل إدارة البيانات بمسؤولية. يمكن أيضًا تطوير هذه التصنيفات كممارسة جماعية لمساعدة المنظمات على التوافق حول ما يشكل البيانات الحساسة في سياقها وتحديد أساليب الإفصاح أو النشر المناسبة لأنواع البيانات المختلفة بناءً على حساسيتها.

تصنيف حساسية المعلومات والبيانات		
الحساسية	التعريف	تصنيف حساسية المعلومات والبيانات
منخفضة أو معدومة	معلومات أو بيانات، إذا تم الكشف عنها أو الوصول إليها بدون تفويض صحيح، من غير المحتمل أن تسبب أي ضرر أو تأثيرات سلبية للأشخاص المتأثرين و/أو العاملين في المجال الإنساني.	**عامة**
متوسطة	معلومات أو بيانات، إذا تم الكشف عنها أو الوصول إليها بدون تفويض صحيح، من المحتمل أن تسبب ضررًا طفيفًا أو تأثيرات سلبية و/أو تكون غير ملائمة للأشخاص المتأثرين و/أو العاملين في المجال الإنساني.	**مقيدة**
عالية	معلومات أو بيانات، إذا تم الكشف عنها أو الوصول إليها بدون تفويض صحيح، من المحتمل أن تسبب ضررًا خطيرًا أو تأثيرات سلبية للأشخاص المتأثرين و/أو العاملين في المجال الإنساني و/أو أضرارًا للاستجابة.	**سرية**
شديدة	معلومات أو بيانات، إذا تم الكشف عنها أو الوصول إليها بدون تفويض صحيح، من المحتمل أن تسبب ضررًا شديدًا أو تأثيرات سلبية و/أو أضرارًا للأشخاص المتأثرين و/أو العاملين في المجال الإنساني و/أو تعيق سير العمل في الاستجابة.	**سرية للغاية**

الشكل ١. نموذج لتصنيف حساسية المعلومات والبيانات[٦]

[٥] لا ينبغي مشاركة البيانات الشخصية بشكل مفتوح، ويجب أن يتوافق إدارة البيانات الشخصية دائمًا مع القوانين الوطنية والإقليمية لحماية البيانات، أو مع سياسات حماية البيانات الداخلية في حالة المنظمات المشمولة بالامتيازات والحصانات.

[٦] UNOCHA (2019), Working Draft Data Responsibility Guidelines.

تشمل السياسات التنظيمية وأدوات الحوكمة الجماعية مثل بروتوكولات مشاركة المعلومات (ISPs) غالبًا تصنيفًا للحساسية ويجب أن تكون النقاط الرئيسية المرجعية لتحديد كيفية إدارة البيانات الحساسة. ومع ذلك، تميل هذه الوثائق إلى ترك مساحة للتقدير فيما إذا كان يجب المشاركة وكيفية القيام بذلك. هذا يعني أن مشاركة البيانات يمكن أن تتأثر بالتفضيلات والمهارات الشخصية وقد تختلف عبر المنظمات. من خلال اتباع نهج أكثر اتساقًا لمشاركة البيانات وضمان حماية كافية للبيانات الحساسة، يمكن للمنظمات بناء الثقة والمساهمة في استجابة إنسانية أكثر كفاءة وفعالية.

أربعة عوامل لتحديد ما إذا كان يجب مشاركة البيانات غير الشخصية

هناك أربعة عوامل يجب على المنظمات الإنسانية أخذها في الاعتبار عند اتخاذ قرار مشاركة البيانات غير الشخصية:

١. ما هي فائدة البيانات لأصحاب المصلحة الآخرين؟
تعتمد فائدة البيانات على مستوى التفاصيل، وعدد الأشخاص أو المنطقة الجغرافية التي تغطيها، وتوقيتها، وأهميتها للتحليل واتخاذ القرار في الاستجابة الإنسانية. يمكن إجراء تقييم تأثير البيانات (DIA) للمساعدة في تحديد فائدة البيانات المحددة.[٧]

٢. مدى حساسية البيانات؟
تعتمد حساسية البيانات على المخاطر المرتبطة بكشفها في سياق معين.[٨] في بعض سياقات الاستجابة، لدى المنظمات والقطاعات والهياكل التنسيقية على مستوى النظام تصنيفات لحساسية البيانات والمعلومات (انظر أعلاه) التي يمكن أن تُعلم هذا التحديد. يمكن أن يساعد إجراء تقييم تأثير البيانات أيضًا في تحديد حساسية البيانات. بالنسبة لنتائج الاستطلاعات وأشكال البيانات الدقيقة الأخرى، تكون الحساسية مرتبطة بشكل وثيق بخطر إعادة التحديد، والذي يمكن تحديده عن طريق تطبيق تقييم مخاطر الإفصاح.

٣. ما هي القدرات البشرية والتقنية للمنظمات التي تشارك وتستخدم البيانات؟
يجب أن تكون كل من المنظمة التي تشارك البيانات والمنظمات التي تستلم وتستخدم البيانات تمتلك قدرات بشرية وتقنية كافية لإدارة البيانات بمسؤولية.[٩] يشمل ذلك توافر الموظفين، ومحو الأمية البياناتية، والبنية التحتية التقنية والموارد ذات الصلة. في البيئات ذات الاتصال المنخفض، قد لا تكون طرق مشاركة البيانات الثقيلة بالنطاق الترددي مناسبة. في السياقات التي تعرف مخاطر أمنية، يجب عادةً مشاركة البيانات من خلال نهج أكثر تحديدًا.

٤. ما هي أدوات الحوكمة التي تنطبق؟
تشمل أدوات حوكمة البيانات الشائعة ISPs، واتفاقيات مشاركة البيانات للمشاركة الثنائية للبيانات، والتراخيص أو شروط الاستخدام لمشاركة البيانات العامة. يجب أن تُعلم هذه الأدوات كيفية مشاركة البيانات بطريقة آمنة وأخلاقية وفعالة. في بعض الحالات، ستحتاج الحوكمة إلى التطوير للنهج المختار لمشاركة البيانات. يمكن لأدوات الحوكمة معالجة مجموعة من المواضيع والأحكام الخاصة، ولكن يجب أن تشمل دائمًا العناصر التالية: (أ) الغرض والنطاق من المشاركة؛ (ب) أي قيود على كيفية إدارة البيانات بعد المشاركة؛ (ج) الأدوار والمسؤوليات طوال عملية المشاركة؛ و(د) إجراءات إدارة حوادث البيانات.[١٠]

[٧] انظر مذكرة التوجيه حول تقييم تأثير البيانات.
[٨] في إدارة البيانات في القطاع الإنساني، يمكن تعريف المخاطر على أنها احتمال وتأثير الضرر الناتج عن إدارة البيانات.
[٩] التراخيص الموصى بها لمشاركة البيانات عبر HDX مدرجة هنا: https://data.humdata.org/about/license.
[١٠] لمزيد من المعلومات حول إدارة حوادث البيانات في الاستجابة الإنسانية، انظر مذكرة التوجيه حول إدارة حوادث البيانات.

تحديد ومقارنة النهج

يجب على المنظمات تحديد أفضل نهج لمشاركة البيانات بناءً على العوامل الأربعة المذكورة أعلاه. تتراوح هذه النهج من المشاركة المفتوحة لتحقيق أقصى فائدة من البيانات، إلى النهج الأكثر تحديدًا مثل المشاركة الثنائية للبيانات أو مشاركة رؤى البيانات فقط. يحتوي الجدول أدناه على نظرة عامة على النهج المختلفة لمشاركة البيانات ويقدم أمثلة لبعض الأدوات والمنصات الشائعة الاستخدام.

نُهُج وأدوات ومنصات مشاركة البيانات في الاستجابة الإنسانية[١١]				
نَهُج المشاركة	**الوصول المفتوح** مشاركة البيانات علنًا	**الوصول المحدود** يسمح الوصول المحدود للبيانات للشركاء المحددين باستخدام البيانات طالما أنهم يستوفون متطلبات معينة.	**المشاركة الثنائية** المشاركة الثنائية هي الطريقة الأكثر تحديدًا لمشاركة البيانات، مباشرة مع شريك واحد.	**عدم مشاركة البيانات** البيانات التي لا ينبغي مشاركتها على الإطلاق يمكن أن توفر قيمة للشركاء إذا تم السماح لهم بالاستفسار عن
الأدوات والمنصات الشائعة	منصات بيانات المنظمات HDX قوائم البريد المفتوحة	HDX الخاص مكتبة البيانات الدقيقة للمفوضية السامية للأمم المتحدة لشؤون اللاجئين (UNHCR)[١٢] IFRC GO[١٣] مشاركة القطاعات/ المجموعات قوائم البريد المغلقة	HDX Connect البريد الإلكتروني[١٤] Dropbox	OPAL[١٥] Aircloak[١٦] التشفير المتماثل[١٧] الحساب متعدد الأطراف[١٨]

عند مقارنة هذه النُهُج المختلفة، يجب دائمًا النظر في النهج الأكثر انفتاحًا أولاً والعمل نحو النهج الأكثر تحديدًا حسب الضرورة. تتطلب أنواع البيانات المختلفة طرقًا مختلفة للمشاركة. على سبيل المثال، ستتطلب الملفات الكبيرة بنية تحتية متخصصة، وتعتبر واجهات برمجة التطبيقات (APIs) مناسبة للبيانات التي يتم نشرها بنفس التنسيق بشكل منتظم. نظرًا لأن تقنيات مشاركة البيانات تستمر في التطور، ينبغي على المنظمات مراجعة ومقارنة نُهُج مشاركة البيانات المتاحة بانتظام.

[١١] ليس جميع الأدوات والمنصات في هذه النظرة العامة قد تم التحقق منها من قبل أمانة الأمم المتحدة. دائمًا استشر مستشاري تكنولوجيا المعلومات المعنيين قبل استخدام أداة جديدة.

[١٢] مكتبة البيانات الدقيقة التابعة للمفوضية السامية للأمم المتحدة لشؤون اللاجئين.

[١٣] منصة IFRC GO.

[١٤] في الاستجابات الإنسانية، إحدى الطرق الأكثر شيوعًا لمشاركة البيانات هي عبر مرفقات البريد الإلكتروني. عند مشاركة البيانات عبر البريد الإلكتروني، تأكد دائمًا من اتخاذ الاحتياطات الأمنية اللازمة. قد تكون هذه الطريقة مسؤولة في بعض الحالات، ولكن هناك غالبًا طرق أكثر ملاءمة لمشاركة البيانات. لمزيد من المعلومات حول كيفية تشفير البريد الإلكتروني، انظر على سبيل المثال: (https://www.cloudwards.net/how-to-encrypt-your-emails/).

[١٥] مشروع الخوارزميات المفتوحة.

[١٦] Aircloak Insights.

[١٧] لمعرفة المزيد عن التشفير المتماثل كطريقة لمشاركة قيمة البيانات الحساسة، انظر هنا: [مشروع التشفير المتماثل من مايكروسوفت] (https://www.microsoft.com/en-us/research/project/homomorphic-encryption/) وهنا: (https://www.wired.com/story/google-private-join-compute-database-encryption/).

فتح القيمة من البيانات دون مشاركتها: نهج الاستعلام

نهج حديث نسبيًا لاستخدام البيانات دون نقلها هو "الاستعلام". يسمح الاستعلام للأطراف الثالثة بصياغة أسئلة محددة ليتم طرحها على البيانات دون الوصول إليها مباشرة. يمكن بعد ذلك التحقق من النتائج الحساسة وأي قضايا أخرى من قبل حامل البيانات. يتجنب هذا النهج عمليات نقل البيانات التي يمكن أن تسبب قضايا قانونية وأخلاقية، بينما يسمح بالاستفادة من رؤى قيمة للصالح العام.

عند تنفيذ نهج الاستعلام، من الضروري إنشاء حوكمة في شكل تعليمات وحدود بشأن الاستفسارات التي يمكن إرسالها، لمنع استرجاع المعلومات الحساسة من خلال طرح مجموعة من الأسئلة. يجب دائمًا أن يكون تقييم المستخدمين وكذلك أسئلتهم خطوة رئيسية في العملية حول هذا النوع من النهج.

تشمل الحلول التجارية لإعداد نهج الاستعلام Aircloak Insights، التي تعمل كـ "وسيط بين المحللين والبيانات الحساسة التي يحتاجون للعمل معها." أداة استعلام أخرى هي منصة Open Algorithms (OPAL). تم تطوير هذه الأداة خصيصًا لقطاعي الإنساني والتنمية وتُجرب حاليًا في كولومبيا.

طرق مشاركة البيانات في خدمة التوصيف المشترك للنازحين

في عام ٢٠١٩، حصلت خدمة التوصيف المشترك للنازحين (JIPS) على منحة من صندوق الابتكار التابع للمفوضية السامية للأمم المتحدة لشؤون اللاجئين (UNHCR) للبحث في طرق علم البيانات المتقدمة لإخفاء هوية البيانات. درست JIPS طرقًا مثل الحساب متعدد الأطراف والتشفير المتماثل وعملت مع خبراء تقنيين في مختبر الفيزياء التطبيقية بجامعة جونز هوبكنز، و Flowminder ومكتب الإحصاءات الوطنية في حكومة كولومبيا.

بالتعاون الوثيق مع Flowminder وبناءً على Flowkit الخاص بهم، طورت JIPS نموذجًا أوليًا لنهج الاستعلام لتمكين الجهات الفاعلة الإنسانية والتنموية من الوصول الآمن إلى البيانات الحساسة على مستوى الأفراد واستعلامها دون الحاجة إلى مشاركتها. طورت الفريق سير عمل تقني لإثبات جدوى هذا النهج مع مزود بيانات واحد ورسم المشكلات والقيود في حالة وجود مزودين متعددين للبيانات.

يُشجَّع المنظمات على مشاركة تجربتها في تعزيز مسؤولية البيانات في تصميم وتنفيذ AAP مع المركز عبر البريد الإلكتروني: centrehumdata@un.org.

المتعاونون: خدمة التوصيف المشترك للنازحين (JIPS).

ينشر مركز البيانات الإنسانية ("المركز")، بالتعاون مع الشركاء الرئيسيين، سلسلة من ثماني مذكرات إرشادية حول مسؤولية البيانات في العمل الإنساني خلال عامي ٢٠١٩ و٢٠٢٠. تتبع سلسلة المذكرات الإرشادية نشر إرشادات مسؤولية البيانات لمكتب تنسيق الشؤون الإنسانية في مارس ٢٠١٩. من خلال هذه السلسلة، يهدف المركز إلى تقديم إرشادات إضافية حول القضايا والعمليات والأدوات المحددة لمسؤولية البيانات في الممارسة العملية. تم تمكين هذه السلسلة بفضل الدعم السخي من المديرية العامة للحماية المدنية وعمليات المساعدة الإنسانية الأوروبية (DG ECHO).

يغطي هذا المستند أنشطة المساعدات الإنسانية المنفذة بمساعدة مالية من الاتحاد الأوروبي. لا ينبغي بأي شكل من الأشكال اعتبار الآراء الواردة هنا تعبيرًا عن الرأي الرسمي للاتحاد الأوروبي، كما أن المفوضية الأوروبية ليست مسؤولة عن أي استخدام قد يتم للمعلومات التي يحتويها.

هذا المشروع ممول جزئيًا
من الاتحاد الأوروبي

[١٨] لمعرفة المزيد عن الحساب متعدد الأطراف، انظر هنا:
https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/data-sharing/secure-multi-party-computation/.

[١٩] للحصول على شرح لهذا الخطر، انظر على سبيل المثال:
https://www.usenix.org/conference/usenixsecurity19/presentation/gadotti.