CaLP
The Cash Learning Partnership

مجموعة أدوات مسؤولية البيانات

دليل لممارسي المساعدات النقدية والقسائم

جدول المحتويات والشكر والتقدير

جدول المحتويات

الشكر والتقدير

تم إجراء مجموعة أدوات مسؤولية البيانات – دليل لممارسي المساعدات النقدية والقسائم هذا بواسطة شراكة التعلم النقدي بتمويل من وزارة الخارجية الفيدرالية الألمانية.

أجرت ليندا رافتري، مستشارة مستقلة، البحث الخاص بهذا المنشور بين حزيران وأيلول 2020.

تم تطوير المنشور بواسطة ليندا رافتري (@meowtree)، مع الإشراف التحريري والمحتوى والدعم من قبل آنا كونداكتشيان (@akondakhchyan) من شراكة التعلم النقدي. استفاد هذا العمل التعاوني من مدخلات لا تقدر بثمن من العديد من المنظمات وممارسي المساعدات النقدية والقسائم، الذين ساهموا بأفكارهم ووقتهم في عملية البحث من خلال مقابلات المبلغين الرئيسيين ومصادر البيانات.

نتوجه بشكر خاص إلى أعضاء اللجنة الاستشارية على دعمهم الحاسم في توجيه تطوير مجموعة الأدوات ومراجعة المسودات. الأعضاء هم: آموس دورنبوس (وورلد فيجين انترناشونال)، جيمس ايتون لي (اوكسفام)، ستيوارت كامبو (OCHA HDX)، جيني كاسويل (GSMA)، جو بيرتون (ICRC)، غابرييلا ايربا (اليونيسيف) وروزا أكباري (ميرسي كوربس).

إن الآراء الواردة في هذا المنشور هي آراء المؤلفين وحدهم وليست بالضرورة آراء المانحين أو الوكالات الأعضاء في شراكة التعلم النقدي.

إن شراكة التعلم النقدي هي شبكة عالمية ديناميكية تضم أكثر من 90 منظمة تعمل في المجالات الحساسة للسياسة والممارسة والبحث في المساعدات النقدية والقسائم الإنسانية والمساعدات المالية على نطاق أوسع.

لمزيد من المعلومات يرجى زيارة موقع شراكة التعلم النقدي: www.calpnetwork.org

تابع شراكة التعلم النقدي على تويتر: @calpnetwork

تمهيد

بينما تجمع جميع البرامج الإنسانية كميات كبيرة من البيانات؛ فإننا في المساعدة النقدية والقسائم نجمع كميات كبيرة من البيانات التي غالبًا ما تتم مشاركتها مع جهات فاعلة متعددة. الكثير من البيانات التي نجمعها حساسة للغاية وذات خصوصية، حيث أننا نجمعها من وحول الأشخاص المهمشين. من المهم تصميم برامجنا وإدارة البيانات بطرق تقلل من احتمالية استخدام هذه البيانات - عن طريق الخطأ أو بشكل مقصود - بطرق تسبب ضرراً أو تستبعد بشكل غير عادل أفراد أو مجموعات معينة من المنافع.

تشمل أنواع الضرر المرتبط بالبيانات والتقنيات الرقمية:

- **خطر الإصابة**، على سبيل المثال؛ عند استخدام البيانات لتحديد والتسبب على وجه التحديد بضرر جسدي أو عاطفي أو نفسي لفرد أو مجموعة[1]
- **الحرمان من الخدمات أو التمييز** على أساس البيانات، بما في ذلك خسائر الفرص والخسائر الاقتصادية عند استخدام البيانات لاتخاذ قرارات بشأن من هو المؤهل للحصول على خدمات أو مزايا معينة[2]
- **انتهاكات حقوق الإنسان؛** مثل فقدان الكرامة أو الحرية أو الخصوصية عند استخدام البيانات بطرق تجرد الأفراد من إنسانيتهم أو عندما يتم اتخاذ القرارات عن طريق خوارزميات الحاسوب أو عندما يتم جمع البيانات ومعالجتها ومشاركتها دون إذن، أو عندما يتعين على الأفراد التخلي عن بياناتهم مقابل خدمة منقذة للحياة أو للحصول على حق آخر[3]
- **الاستهداف المتعمد والتحرش** بالفقراء من خلال التقنيات الحديثة. كما لوحظ في تقرير المقرر الخاص بشأن التقنيات الرقمية وحالة الرفاهية؛ فإن استخدام التقنيات لتحديد الاحتيال أو انتهاكات الشروط المفروضة على المستفيدين عندما يتلقون نقودًا أو مزايا رعاية اجتماعية أخرى تسمح بجمع المعلومات رقمياً وتخزينها لفترة زمنية غير محددة، وهذا يعني أنه يتم الاحتفاظ بكميات هائلة من المعلومات ويمكن استخدامها ضد شخص ما إلى أجل غير مسمى[4]
- **تدهور الهيكليات الاجتماعية أو الديمقراطية،** على سبيل المثال؛ من خلال التلاعب أو تضخيم اختلالات القوة أو المعلومات المضللة[5]

تعد إدارة البيانات ومشاركة المعلومات من المكونات الحاسمة للمساعدات النقدية والقسائم؛ حيث أننا نعمل مع البيانات الحساسة طوال عملية المساعدات النقدية والقسائم بأكملها. لذلك، فبالطريقة نفسها التي تعتبر فيها الحماية و "عدم إلحاق الضرر" بمثابة أجزاء أساسية من المساعدات النقدية والقسائم وغيرها من البرامج الإنسانية؛ يجب دمج مسؤولية البيانات في كل ما نقوم به كممارسين في المساعدات النقدية والقسائم. بينما تعتبر مجموعة الأدوات هذه موجهة نحو المساعدات النقدية والقسائم؛ إلا أن الكثير من الإرشادات يمكن أن تمتد إلى البرامج الإنسانية الأخرى أيضاً.

الصندوق 1: ما هي مسؤولية البيانات؟

تتجاوز مسؤولية البيانات خصوصية البيانات وحماية البيانات لتشمل المبادئ والعمليات والأدوات التي تدعم الإدارة الآمنة والأخلاقية والفعالة للبيانات.

---

1 راجع إطار عمل "أنواع الضرر" من مايكروسوفت للحصول على نظرة أعمق

2 انظر ألستون، ب. (2019) "تقرير المقرر الخاص المعني بالفقر المدقع وحقوق الإنسان" والذي يستعرض دور التقنيات الرقمية ودولة الرفاهية. تم تقديمها في الدورة الرابعة والسبعين للجمعية العامة للأمم المتحدة حول موضوع تعزيز وحماية حقوق الإنسان: مسائل حقوق الإنسان، بما في ذلك النهج البديلة لتحسين التمتع الفعلي بحقوق الإنسان والحريات الأساسية

3 انظر اللائحة العامة لحماية البيانات (2018) التي تسرد حقوق صاحب البيانات بما في ذلك الحق في رفض معالجة البيانات والحق في عدم التوصيف بالبيانات والحق في عدم اتخاذ قرارات آلية تؤثر على حياة الفرد بالإضافة إلى الحق في الطعن في القرارات الآلية والمطالبة بمراجعتها من قبل إنسان

4 ألستون 2019

5 إطار عمل "أنواع الضرر" من مايكروسوفت

6 مكتب تنسيق الشؤون الإنسانية (2016) "التفكير بإيجاز: بناء مسؤولية البيانات في العمل الإنساني"

نقاط رئيسية لأخذها بعين الاعتبار:

- **تتعلق مسؤولية البيانات بأكثر من مجرد بيانات.** كما هو الحال مع البضائع القيّمة الأخرى؛ فقد أصبحت البيانات سلعة. عادةً ما يتم تحويل نقاط البيانات الفردية إلى معلومات قيمة يتم استخدامها من قبل جهات فاعلة مختلفة لجميع أنواع الأغراض - تلك التي تساعد وتلك التي تضر. لقد نشأ نظام بيئي كامل حول البيانات التي تم جمعها ومعالجتها من خلال المساعدات النقدية والقسائم. يمكن أن تمنح البيانات القوة والمزايا الاقتصادية للأفراد والوكالات الإنسانية والحكومات المحلية والوطنية ومقدمي الخدمات المالية والمراقبين الخارجيين وشركات التكنولوجيا والجهات الفاعلة غير الحكومية، وجميعهم يتعاملون مع البيانات في المساعدات النقدية والقسائم
- **تتطلب مسؤولية البيانات التوفيق بين السياق والإبداع والقدرة والتعاون،** حيث تقوم مجموعة متنوعة من الجهات الفاعلة بجمع البيانات وإدارتها واستخدامها ومشاركتها في المساعدات النقدية والقسائم. هناك اختصاصات ودوافع تنظيمية مختلفة وديناميكيات القوة ومستويات المهارات والمعرفة في العملية، حيث ستحتاج إلى إيجاد طرق مرنة وقابلة للتكيف للتخفيف من المخاطر والأضرار المرتبطة بالبيانات، لا سيما في السياقات المتأثرة بالنزاع أو الهشة. ستعتمد مسؤولية البيانات على كل فرد مشارك في دورة البرنامج، من مسؤولي التعداد الأفراد وموظفي الخطوط الأمامية من خلال فرق الإدارة القطرية ومقدمي الخدمات المالية والشركاء والمانحين، وفي بعض الأحيان، يمكن أن تعرّض حماية البيانات العاملين في المجال الإنساني والعاملين في الخطوط الأمامية للخطر أيضاً
- **لا تعد مسؤولية البيانات نشاطاً منفرداً - فهي تتطلب فرقًا بتدوير جيد،** حيث ستحتاج إلى إشراك أجزاء مختلفة من مؤسستك وأنواع متعددة من الخبرة أثناء التفكير في كيفية ضمان حماية البيانات والتخفيف من الأضرار المحتملة المتعلقة بالبيانات في المساعدات النقدية والقسائم، وسيتطلب ذلك مهارات تقنية مثل أمن المعلومات وإدارة أنظمة البيانات وتحليل البيانات والهندسة المعمارية والإدارة القانونية والتجارية والامتثال وفهم التمويل والنوع الاجتماعي والإدماج والحماية والوقاية والمهارات الشخصية مثل التفاوض وبناء توافق الآراء

في مجموعة الأدوات هذه؛ فإننا نقدم مجموعة من الطرق للعمل بمسؤولية البيانات في أنشطة تخطيط البرامج وتصميمها وتنفيذها والمراقبة والتقييم والمساءلة والتعلم. تقدم مجموعة الأدوات معياراً ذهبياً يجب على المؤسسات أن تطمح إليه وتحدد الآثار القانونية والأخلاقية التي يجب أن نضعها في الاعتبار عند معالجتنا للبيانات. نحن ندرك أنه لن يكون من الممكن دائمًا تحقيق المعيار الذهبي، حيث ستكون هناك دائماً مفاضلات من حيث السرعة والميزانية وعوامل أخرى يجب مراعاتها، ونحن نعلم أن ممارسي المساعدات النقدية والقسائم سيتم جذبهم في اتجاهات عديدة. في الحالات التي تكون فيها قدرتنا المؤسسية أقل بكثير من المعايير القانونية والأخلاقية، ومع ذلك قد نحتاج إلى وقف الأنشطة لأن جمع البيانات لدينا قد يؤدي إلى ضرر أو لأن ذلك قد يخرق القانون.

البيانات هي امتداد للشخص، ويجب أن نتعامل مع بيانات الشخص بنفس الاحترام والرعاية التي نتعامل بها مع الشخص الطبيعي كما لو أنه يقف أمامنا.

لم يجب أن تكون هناك مجموعة أدوات أخرى؟

في عام 2016 أنتجت ELAN مجموعة Data Starter Kit [7] وهي واحدة من أقدم مجموعات الأدوات للتعامل مع موضوع مسؤولية البيانات في القطاعات الإنسانية والتنموية، حيث كانت Data Starter Kit مصدراً أساسياً لمجتمع شراكة التعلم النقدي وعلى نطاق أوسع بواسطة الممارسين المسؤولين عن البيانات حول العالم. نظراً لتغير عالم المساعدات النقدية والقسائم منذ عام 2016، شعرت شراكة التعلم النقدي أنه من الضروري تحديث Data Starter Kit لتلبية الأوقات الحالية. ارتفع الحجم الهائل للمساعدات النقدية والقسائم من 2.8 مليار دولار في عام 2016 إلى 5.6 مليار دولار في عام 2019، ما يعني أن المساعدات النقدية والقسائم تشكل الآن حوالي 18% من إجمالي المساعدات الإنسانية الدولية.[8]

لقد كان هناك أيضاً تركيز متزايد على الجودة وتمر المساعدات النقدية والقسائم بتحول في الأدوار والشراكات، حيث تتطلب المساعدات النقدية والقسائم بشكل متزايد التنسيق بين شركاء متعددين من أجل الوصول إلى النطاق والاستدامة. يتم التنسيق مع أصحاب المصلحة بين مختلف الوزارات الحكومية ووكالات الأمم المتحدة وحركة الصليب الأحمر والهلال الأحمر والمنظمات الدولية غير الحكومية والمنظمات المحلية بالإضافة إلى كل من أنظمة البيانات الخاصة بها. تشمل المساعدات النقدية والقسائم العديد من الشركاء وغالباً ما يتطلب من الشركاء المنفذين استخدام أنظمة كبيرة وراسخة ويقترح العديد منهم دمج الهوية الرقمية (المعرف الرقمي) أو القياسات الحيوية لتحديد الهوية. تعتمد المساعدات النقدية والقسائم بشكل متزايد على الوسائل الرقمية، لذلك من المرجح أن تشارك البنوك ومشغلي شبكات الهاتف المحمول ومؤسسات التمويل الأصغر ومجموعة متنوعة من مزودي التكنولوجيا المالية الجدد.

7 ELAN (2016) "مجموعة أدوات البيانات الأولي".
8 شراكة التعلم النقدي (2020) "حالة النقد في العالم 2020"

الصندوق 2: ما هو النظام الأوروبي العام لحماية البيانات؟

دخل النظام الأوروبي العام لحماية البيانات الخاص بالاتحاد الأوروبي حيز التنفيذ في أيار 2018، وهو يعتبر بشكل عام أقوى نظام لخصوصية البيانات في العالم. تلتزم معظم المنظمات التي تتخذ من الاتحاد الأوروبي مقراً لها بالامتثال للنظام الأوروبي العام لحماية البيانات وتقوم العديد من البلدان في أجزاء أخرى من العالم بوضع أنظمة الخصوصية الوطنية الخاصة بها على النظام العام لحماية البيانات، حيث أن الأمم المتحدة واللجنة الدولية للصليب الأحمر غير ملزمتين بالنظام الأوروبي العام لحماية البيانات لأن لديهما امتيازات وحصانات معينة بسبب مكانة منظماتهما الدولية.

يتزايد حجم البيانات التي يتم جمعها وتخزينها واستخدامها ومشاركتها عبر شركاء المساعدات النقدية والقسائم باستمرار، وفي الوقت نفسه، يتم تطوير قوانين خصوصية البيانات الجديدة والمحدثة مثل النظام الأوروبي العام لحماية البيانات الخاص بالاتحاد الأوروبي وإنفاذه في البلدان حول العالم، حيث تضع هذه القوانين متطلبات جديدة للمنظمات التي تدير البيانات الشخصية وغيرها من أشكال البيانات الحساسة، كما يتزايد أيضاً الوعي بأهمية إدارة البيانات بأمان وواجبنا في الرعاية ومسؤولية حماية المشاركين في البرنامج والالتزام بعدم إلحاق الضرر بالبيانات.

في ظل هذه المعلومات العامة؛ نقدم طياً مجموعة أدوات محدثة لمسؤولية البيانات لتعكس هذه التغييرات الواسعة.

الصندوق 3: ما أنواع البيانات التي تغطيها مجموعة الأدوات؟

يشمل مصطلح "البيانات" في الوثائق الإرشادية هذه (بالاستعارة من OCHA[9] و ICRC[10]) كلاً من البيانات الحساسة وغير الشخصية، بما في ذلك:

1. بيانات عن الأشخاص المتأثرين بأزمة واحتياجاتهم (على سبيل المثال؛ البيانات الشخصية لمتلقي المساعدات النقدية والقسائم)
2. بيانات حول السياق الذي تحدث فيه الأزمة (على سبيل المثال؛ معلومات عن المجتمعات التي تتلقى المساعدات النقدية والقسائم)
3. بيانات حول استجابة المنظمات والأشخاص الذين يسعون للمساعدة (على سبيل المثال؛ مواقع توزيع النقد أو خطط تمارين جمع البيانات)

البيانات الشخصية هي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه.

البيانات الحساسة هي البيانات التي إذا تم الكشف عنها أو الوصول إليها دون تصريح مناسب، يمكن أن تؤدي إلى:

- الضرر (مثل العقوبات والتمييز والتهديدات الأمنية) لشخص ما بما في ذلك مصدر المعلومات أو الأشخاص أو المجموعات الأخرى التي يمكن التعرف عليها
- تأثير سلبي على قدرة المنظمة على تنفيذ أنشطتها أو على التصورات العامة لتلك المنظمة

سيكون للبيانات مستويات متفاوتة من الحساسية اعتمادًا على السياق؛ لذلك لم نقدم قائمة محددة بنقاط البيانات الحساسة في هذا الدليل.

9 مكتب تنسيق الشؤون الإنسانية (2019) "إرشادات مسؤولية البيانات: مسودة عمل"
10 اللجنة الدولية للصليب الأحمر (2020) "دليل حماية البيانات"

كيف تمت هيكلة مجموعة الأدوات؟

نستعرض في مجموعة الأدوات هذه البيانات المسؤولة في المساعدات النقدية والقسائم من منظور دورة حياة البيانات، وتجدر الإشارة إلى أن دورة حياة البيانات ليست حلقة واحدة؛ بل هي رسم مرئي يساعد على توجيه التفكير الشامل حول البيانات. نتوقع منك إعادة النظر في دورة حياة البيانات مع تطور برنامجك وتنفيذك لأنشطة بيانات إضافية.

الصندوق 4: دورة حياة البيانات

تعد دورة حياة البيانات مفيدة لتوجيه أنشطة البيانات الكلية للاستجابة الكاملة ولأنشطة جمع البيانات الفردية في مراحل مختلفة من الاستجابة. (دورة الحياة المستخدمة هنا توضيحية، وقد يكون لدى المؤسسات نسختها الخاصة من دورة حياة البيانات).

لسهولة الاستخدام؛ تم تقسيم مجموعة الأدوات هذه إلى 7 وثائق إرشادية تتناول قضايا السياق والقدرة المؤسسية والتصميم والتخطيط والتنفيذ. تغطي الوثائق الإرشادية باختصار:

السياق والقدرة المؤسسية (الوثيقة الإرشادية 1)

يجب اتخاذ قرارات رفيعة المستوى في وقت مبكر حول ما إذا كانت المنظمات لديها القدرة على تنفيذ المساعدات النقدية والقسائم بشكل آمن وأخلاقي، وهذا يشمل تقييم المشهد العام للبيانات والسياق القطري والسياق القانوني وديناميكيات السلطة المرتبطة بالبيانات في المساعدات النقدية والقسائم.، كما يشمل أيضاً تقييماً لجوانب الامتثال وعلاقات البيانات والأنظمة التي سيتم استخدامها (وغالباً ما تكون مطلوبة) من قبل الجهات المانحة والاتحادات ووكالات الأمم المتحدة وحركة الصليب الأحمر والهلال الأحمر والمنظمات غير الحكومية الدولية والوطنية والحكومات ومقدمي الخدمات المالية والشركاء الآخرين في برامج المساعدات النقدية والقسائم. يشمل تقييم القدرات المؤسسية في هذه المرحلة المهارات والمعارف والموارد اللازمة لحماية البيانات واستخدام الأدوات والعمليات الرقمية بشكل مسؤول في السياق أعلاه. يمكن دمج العديد من الجوانب التي وضعناها في الوثيقة الإرشادية في دراسات تحليل الوضع واستعداد المساعدات النقدية والقسائم القائم.

الصندوق 5: القانوني مقابل الأخلاقي

عندما تفعل شيئًا قانونيًا، ستسأل هل يمكننا فعل ذلك؟ عند القيام بشيء ما بشكل أخلاقي، سوف تسأل هل يجب علينا القيام بذلك؟ في بعض الأحيان يكون ما هو قانوني غير أخلاقي.

التصميم والتخطيط (الوثيقة الإرشادية 2)

تساعد مرحلة التصميم والتخطيط المؤسسات على وضع نهجها في جمع البيانات بطريقة مسؤولة وإدارتها ضمن المراحل المختلفة لدورة برنامج المساعدات النقدية والقسائم (الاستهداف والمشاركة والتسجيل والتسليم والمراقبة والتقييم والمساءلة والتعلم). من المحتمل أن تتطلب كل مرحلة من مراحل دورة برنامج المساعدات النقدية والقسائم نوعًا من جمع البيانات والتقاطها وإدارتها طوال دورة حياة البيانات. على سبيل المثال، عادة ما يتم إجراء تقييمات الاحتياجات ونقاط الضعف في وقت مبكر لمساعدة الوكالات على فهم الاحتياجات المحددة للسكان المتأثرين، حيث يجب أن توجه هذه التقييمات القرارات اللاحقة بشأن أنسب الطرق النقدية للسياق وكمية وتواتر التحويلات والشراكات وشمول الطرف الثالث والعملية الشاملة من البداية إلى النهاية، بما في ذلك البيانات التي سيتم جمعها والكيفية، وأي الأنظمة سيتم استخدامها لتخزين البيانات وتحليلها. تتوافق الجوانب التي يتم تناولها في هذه المرحلة مع تحليل استجابة المساعدات النقدية والقسائم النموذجي ومراحل تصميم البرنامج.

إدارة البيانات خلال التنفيذ (الوثيقة الإرشادية 3 – 7)

بعد مراحل التصميم والتخطيط، تنتقل الاستجابة إلى التنفيذ. خلال مراحل تنفيذ المساعدات النقدية والقسائم تقوم المنظمات بجمع البيانات من السكان المتأثرين من أجل الاستهداف والمشاركة والتسجيل وتسليم النقد أو القسائم[11]، كما تجري أنشطة المراقبة وجمع التغذية الراجعة من السكان المتأثرين لتحسين المساءلة وتكييف جهود إعداد البرامج، حيث يصبح جمع البيانات أثناء مرحلة التنفيذ أكثر تكرارا وأكثر دقة. قد تتفاقم المخاطر والأضرار بسبب زيادة كميات البيانات الشخصية وغيرها من البيانات الحساسة أو بيانات المجموعة التي تتم إدارتها ومشاركتها، حيث تحتاج الوكالات أيضًا إلى اعتبار ما يحدث لبيانات السكان المتأثرين عند إغلاق برنامج أو تسليمه إلى كيان آخر لإدارته، كما هو الحال عندما يتم نقل برامج المساعدات النقدية والقسائم الإنسانية إلى وكالات الحماية الاجتماعية الحكومية أو شركاء التنمية الآخرين.

يمكن أن يساعد استخدام نهج دورة حياة البيانات لتوجيه عملية جمع وإدارة بيانات البرنامج بشكل عام وتخطيط وتنفيذ عمليات جمع البيانات المحددة وإدارتها في المراحل المختلفة من تنفيذ المساعدات النقدية والقسائم، المؤسسات على تعظيم فوائد البيانات وتحديد المخاطر والأضرار والتخفيف منها أثناء التنفيذ، ويمكن للمؤسسات استخدام الوثائق الإرشادية من 3 إلى 7 لوضع خطط لكل مرحلة من مراحل دورة الحياة ثم العودة لإنهاء تصميم وخطة البيانات الشاملة (الوثيقة الإرشادية 2).

11 تميل البرمجة النقدية إلى إشراك كميات أكبر من جمع البيانات ومعالجة البيانات والتنسيق بين الوكالات ومشاركة البيانات، في حين قد تتضمن مساعدة القسائم مشاركة أقل للبيانات لأنها غالبًا ما تُدار داخليًا وتتطلب مشاركة وتنسيقًا أقل للبيانات مع الجهات الفاعلة الأخرى في مجال المساعدات النقدية والقسائم

قائمة الاختصارات

AAP	المساءلة تجاه السكان المتأثرين
AML	مكافحة غسيل الأموال
CaLP	شراكة التعلم النقدي
CDR	سجل تفاصيل المكالمات
CTM	تدابير مكافحة الإرهاب
CVA	المساعدة النقدية والقسائم
CWG	مجموعة العمل النقدي
DPIA	تقييم أثر حماية البيانات
DPO	مسؤول حماية البيانات
FATF	فريق عمل الإجراءات المالية
FSP	مزود الخدمة المالية
GDPR	النظام العام لحماية البيانات
ICRC	اللجنة الدولية للصليب الأحمر
ID	التعريف
INGO	المنظمة غير الحكومية الدولية
KYC	اعرف عميلك
LI	المصلحة القانونية
MEAL	المراقبة والتقييم والمساءلة والتعلم
MNO	مشغلي شبكات الهاتف المحمول
NGO	المنظمة غير الحكومية
OCHA	منظمة تنسيق الشؤون الانسانية
PEA	تحليل الاقتصاد السياسي
PI	المصلحة العامة
PIA	تقييم أثر السرية
RCRCM	حركة الهلال الأحمر والصليب الأحمر
RBA	تقييم المنافع مقابل المخاطر
SCOPE	نظام تسجيل مستفيدي برنامج الأغذية العالمي
SOP	إجراءات التشغيل القياسية
WFP	برنامج الأغذية العالمي
UN	الأمم المتحدة
UNHCR	المفوضية السامية للأمم المتحدة لشؤون اللاجئين
UNICEF	صندوق الأمم المتحدة للطفولة

الوثيقة الإرشادية 1

تقييم السياق والقدرة

عند التخطيط لبرنامج، بما في ذلك برنامج يتضمن المساعدات النقدية والقسائم؛ تحتاج إلى تقييم السياق العام الذي تعمل فيه وقدرة مؤسستك قبل التعمق في خطة البرنامج التفصيلية. في هذا المستوى المتقدم؛ أنت معنيّ بتحديد ما إذا كان بإمكان مؤسستك تشغيل برنامج ما بشكل آمن وأخلاقي في سياق معين.

يجب أن يتضمن هذا التقييم عالي المستوى مراجعة لالتزاماتك وقدراتك على جمع وإدارة البيانات المطلوبة للبرنامج بشكل مسؤول، ومن المرجح أن يشمل أيضاً التقييمات التنظيمية وتقييمات الجدوى وتحديد نطاق السيولة والخدمات المالية وإلقاء نظرة على استراتيجيات المانحين والاعتبارات الأساسية الأخرى.

تساعد مراجعة السياق والقدرات المتعلقة بالبيانات في هذه المرحلة على ضمان أنه يمكنك جمع البيانات التي تحتاجها ومعالجتها وإدارتها بطريقة مسؤولة لتنفيذ البرنامج وفهم المفاضلات حتى تتمكن من اتخاذ القرارات الأساسية. يمكن أن يساعد التقييم عالي المستوى للمجالات الموضحة أدناه على تحديد ما إذا كنت مستعدًا بشكل مسؤول للمضي قدماً في اقتراح أو استجابة ما، وإذا كانت المخاطر والأضرار المتعلقة بالبيانات (على السكان المتأثرين أو مؤسستك أو شركائك أو موظفيك) في الفحص الأول تفوق الفوائد؛ فيجب عليك إعادة تصميم البرنامج أو إعادة التفاوض بشأنه أو إعادة التفكير فيه قبل الانتقال إلى مرحلة الاقتراح. قد يتم بالفعل تضمين المجالات الرئيسية أدناه في عمليات البحث واتخاذ القرار المعتادة الخاصة بك قبل الاقتراح، ولكننا ندرجها على أي حال لأن المؤسسات غالباً لا تركز بشكل كافٍ على مسؤولية البيانات كجزء من عمليات ما قبل العرض.

حدد المبادئ عالية المستوى التي توجه منهجية المؤسسة

قامت الجهات الفاعلة في المجال الإنساني بالفعل بتطوير أو تبني مجموعات مختلفة من المبادئ التي يمكن أن تساعدك في التفكير عالي المستوى حول مسؤولية البيانات في إعداد برامج المساعدات النقدية والقسائم. قد تتبع منظمتك واحدًا أو أكثر من هذه المبادئ، أو قد تتبع مبادئها الخاصة. يمكن أن تساعدك المبادئ رفيعة المستوى على تحديد "الخطوط الحمراء" على المستوى التشغيلي والتي ترفض مؤسستك تجاوزها والجوانب التي تلعب دوراً في قرارات "المتابعة – عدم المتابعة".

تقدم الوثيقة الإرشادية 1 إرشادات بشأن كيفية تقييم السياق والقدرات المتعلقة بالبيانات قبل الشروع في برنامج المساعدات النقدية والقسائم. ستحدد موارد مؤسستك وقدراتها مدى عمق ودقة نهجك في هذه التقييمات، فحتى لو كانت مواردك محدودة، فمن المهم على الأقل اعتبار كل مجال من هذه المجالات في مجموعة سريعة من التقييمات، حيث قد ينبهك السياق وتقييم القدرات إلى موقف يكون فيه المضي قدماً غير حكيم.

- مبادئ حماية خصوصية المستفيدين والمعايير التشغيلية (2013) من شراكة التعلم النقدي
- مبادئ المدفوعات الرقمية في الاستجابة الإنسانية 2015
- مبادئ الأمم المتحدة لحماية البيانات الشخصية والخصوصية 2018
- مبادئ حماية البيانات للائحة العامة لحماية البيانات الخاصة بالاتحاد الأوروبي 2018
- مبادئ معالجة البيانات للجنة الدولية للصليب الأحمر (2020)، الصفحات 35–43

يجب تضمين المبادئ في عمليات الأعمال؛ وأثناء عملك من خلال مجموعة الأدوات هذه، قم بمراجعة وتحديد المكان الذي تتناسب فيه مبادئ وسياسات مؤسستك مع عملياتك. هل توجد هناك أي مستندات أو خطوات بحاجة للترجمة مثل قوائم التحقق أو أطر عمل تقييم المخاطر أو أدوات الفرز المتعلقة بمسؤولية البيانات، والتي قد تحتاج إلى تضمينها في العمليات الحالية؟ هل هناك أي شخص يمكنك الذهاب إليه للحصول على المشورة عندما يكون لديك أسئلة؟

قد تعتبر بعض المنظمات إنشاء لجنة داخلية لأخلاقيات البيانات تقوم بمراجعة برامج استخدام البيانات الأخلاقية والجوانب الأخلاقية الأخرى، وفيما يلي بعض الإرشادات **لإنشاء لجنة الأخلاقيات** لمراجعة البيانات المسؤولة واستخدام التكنولوجيا.

فهم اقتصاد البيانات السياسي في سياقك التشغيلي

البيانات هي القوة؛ في معظم السياقات الإنسانية، يتمتع الشخص الذي يتحكم في معظم البيانات بأكبر قدر من القوة كما يتحكم في الاستجابة. يمكن أن يعني هذا أن الوكالات تتنافس على البيانات وتضغط من أجل اعتماد أنظمة معينة لمركزية إدارتها. تميل الوكالات التي تمتلك أكبر قدر من البيانات أو تروج لأنظمتها على أنها الوضع الافتراضي إلى أن تكون في وضع أفضل للوصول إلى التمويل، أما الكيانات الفردية التي لديها مجموعات بيانات كبيرة فهي قادرة أيضاً على التفاوض بسهولة أكبر مع السلطات المحلية في الحالات التي يتم فيها دمج المساعدات النقدية والقسائم الإنسانية مع جهود الحماية الاجتماعية الحكومية. في وقت تتضاءل فيه الأموال المخصصة لأعمال الإغاثة؛ تعد البيانات بمثابة مصدر توتر بسبب القوة والتمويل اللذان يمكن أن تمنحهما.

الصندوق 6: ما هو تحليل الاقتصاد السياسي؟

يعد تحليل الاقتصاد السياسي بمثابة طريقة منظمة لفحص ديناميكيات القوة وتأثير القوى الاقتصادية والاجتماعية في سياق معين. تحليل الاقتصاد السياسي هي عملية فهم الديناميكيات السياقية وكيف يمكن للتدخلات المختلفة أو التدخلات المحتملة (بما في ذلك التدخلات الإنسانية) أن تتفاعل مع تلك الديناميكيات وتؤثر عليها، حيث يتضمن التفكير في جوانب مثل:

- التأثيرات التأسيسية (مثل التاريخ أو الجغرافيا)
- تأثير الأحداث والجهات الفاعلة المباشرة (مثل تغييرات القيادة أو الكوارث الطبيعية)
- الإطار المؤسسي (الذي يشمل القوانين الرسمية والممارسات غير الرسمية) الذي يشكل السلوكيات والنتائج الملاحظة

يشجع تحليل الاقتصاد السياسي الممارسين على اعتبار هذه الديناميكيات والحوافز والمصالح والتفكير في الكيفية التي يمكن أن تساعدهم في إثراء الممارسة التشغيلية. قد ترغب الجهات الفاعلة في برنامج مكافحة التطرف العنيف في تغطية البلد أو السياق الإقليمي بالإضافة إلى ديناميكيات القوة والقوى الاقتصادية والاجتماعية التي تلعب دوراً في الاستجابة الإنسانية ، بما في ذلك المساعدات النقدية والقسائم

تهتم الحكومات أيضاً بالبيانات لأسباب مختلفة، حيث يشمل ذلك الاستخدامات المفيدة للبيانات لتحسين البرمجة وصنع القرار وكذلك الاستخدامات الأقل إيجابية مثل التلاعب بقوائم المستفيدين من المساعدات النقدية والقسائم أو التنافس على السلطة مع الجهات الفاعلة غير الحكومية أثناء النزاعات أو الاستهداف الضار للأفراد أو الجماعات. قد يرغب القطاع الخاص ومقدمو الخدمات المالية أيضاً في الوصول إلى البيانات من أجل استهداف العملاء الجدد المحتملين بالمنتجات والخدمات أو إجراء البحث والتطوير لمنتجات جديدة أو تحقيق الدخل من البيانات عن طريق بيعها للآخرين.

يعد فهم الدور الذي تلعبه البيانات في سياق عملك أمراً مهماً لتحديد المخاطر والأضرار المحتملة التي يمكن أن تنجم عن جمع البيانات ومعالجتها ومشاركتها، حيث يمكن أن يساعدك هذا بدوره في إبراز المجالات التي لديك فيها مساحة للتفاوض من أجل مسؤولية أكبر عن البيانات. يعد إجراء "تحليل الاقتصاد السياسي للبيانات فيما يتعلق بالمساعدات النقدية والقسائم بمثابة طريقة لتحديد بعض الديناميكيات الأساسية التي تؤثر على كيفية الوصول إلى البيانات والتحكم فيها. قد يتم إجراء تقييم تنفيذي للبيانات بواسطة مراقب خارجي أو مستشار خارجي أو في بعض الحالات شريك من القطاع الخاص، ويمكن أن تعمل مجموعات العمل النقدية التي تعمل بشكل جيد كمساحة محايدة لمناقشة البرنامج التنفيذي الخاص بالبيانات وللاتفاق على مناهج جماعية للبيانات التي تفيد السكان المتأثرين بدلاً من الأساليب الأكثر ترجيحاً نحو خدمة أجندات وكالات أو حكومات معينة.

12 مينوكال إيه وآخرون (2018) "التفكير والعمل سياسيًا من خلال تحليل الاقتصاد السياسي التطبيقي: دليل للممارسين" USAID.

قد ترغب الوكالات الأقل قوة في إجراء تقييم تنفيذي للبيانات من تلقاء نفسها واستخدامه لوضع استراتيجيات لطرق التنقل في ديناميكيات القوة في مساحة المساعدات النقدية والقسائم، وبدلاً من ذلك يمكن إجراء تقييم تنفيذي للسياق العام الأوسع؛ في هذه الحالة يجب أن يتم تضمين تحليل الاقتصاد السياسي للبيانات كأحد العدسات التحليلية.

الصندوق 7: عينة أسئلة إجراء تحليل الاقتصاد السياسي لبيانات المساعدات النقدية والقسائم[13]

- **الادوار والمسؤوليات.** من هم أصحاب المصلحة الرئيسيين؟ ما هي الأدوار والمهام الرسمية و / أو غير الرسمية للاعبين المختلفين؟ ما هو التوازن بين مختلف الجهات الفاعلة في التحكم في البيانات؟
- **هيكلية الملكية والتمويل:** ما هي هيكلية استجابة المساعدات النقدية والقسائم؟ ما هو التوازن بين الوكالات والحكومات والجهات الفاعلة الأخرى من حيث الوصول إلى البيانات والتحكم فيها؟ كيف يتم تمويل المساعدات النقدية والقسائم ومن قبل من؟ ما هي مصالح أولئك الذين يمولون المساعدات النقدية والقسائم؟ كيف تتأثر بجداول الأعمال الأخرى (على سبيل المثال؛ التقشف والقلق بشأن الاحتيال وتمويل دافعي الضرائب والتحالفات على المستوى العالمي والمصالح الخاصة لبعض البلدان في التنمية أو الأوضاع السياسية في بلدان أخرى)؟ إذا كانت إحدى الوكالات تمتلك وتمول جميع أشكال المساعدات النقدية والقسائم فماذا يعني ذلك بالنسبة لمسؤولية البيانات؟
- **ديناميكيات القوة:** لأي مدى تُمنح السلطة في أيدي أفراد أو وكالات أو مجموعات معينة؟ كيف تسعى مجموعات المصالح المختلفة (مزودي الخدمة المالية ووكالات الأمم المتحدة، و RCRCM والمنظمات الدولية غير الحكومية والمنظمات غير الحكومية وشركات التكنولوجيا والبيانات والسكان المتأثرين والحكومات ووسائل الإعلام والمنظمين وما إلى ذلك) للتأثير على كيفية إدارة البيانات ومن يمكنه الوصول إلى البيانات والتحكم فيها؟
- **الموروثات التاريخية.** ما هو التاريخ الماضي لمختلف الجهات الفاعلة في سياق البرمجة هذا أو البلد؟ ما هي العلاقات التاريخية بين مختلف الفاعلين؟ كيف يؤثر هذا على التصورات الحالية لأصحاب المصلحة؟
- **الفساد والبحث عن الريع:** هل يوجد فساد كبير واحتيال وبحث عن الريع في القطاع الإنساني أو برامج المساعدات النقدية والقسائم أو في البلد ككل؟ ما هو دور البيانات في هذا؟ أين ينتشر هذا (على سبيل المثال؛ عند الاستهداف، المشاركة، التسليم، الشراء)؟ من الذي يستفيد أكثر من هذا؟ كيف يتم استخدام المحسوبية؟
- **تسليم المساعدات النقدية والقسائم:** من هم المستفيدون الأساسيون من تسليم المساعدات النقدية والقسائم؟ هل هناك مجموعات اجتماعية أو إقليمية أو عرقية معينة مشمولة و / أو مستبعدة؟ هل يتم تقديم الدعم وما هي الفئات التي تستفيد منها أكثر من غيرها؟
- **الأيديولوجيات والقيم:** ما هي الأيديولوجيات والقيم السائدة التي تشكل وجهات النظر حول القطاع الإنساني أو المساعدات النقدية والقسائم؟ إلى أي مدى يمكن أن تعمل في التأثير على كيفية تقديم المساعدات النقدية والقسائم؟
- **صنع القرار:** كيف تُتخذ القرارات داخل قطاع العمل الإنساني أو في إطار المساعدات النقدية والقسائم؟ من هو الطرف في عمليات صنع القرار هذه؟
- **قضايا التنفيذ:** بمجرد اتخاذ القرارات، هل يتم تنفيذها؟ أين تكمن الاختناقات الرئيسية في النظام؟ هل يرجع الفشل في التنفيذ إلى نقص القدرات أو لأسباب اقتصادية سياسية أخرى؟
- **إمكانية الإصلاح:** من المحتمل أن يكون "الفائز" و"الخاسر" من قرارات معينة حول الوصول إلى البيانات والتحكم فيها؟ من الذي يحتمل أن يقاوم النظام الحالي ومن الذي سيقاوم التغيير ولماذا؟ ما الذي يمكن التفاوض عليه للتغلب على هذه المعارضة؟

اعتماداً على الموقف، يمكنك إجراء تحليل الاقتصاد السياسي بشكل أكثر رسمية (على سبيل المثال عن طريق تعيين طرف ثالث أو الاتفاق مع الشركاء على إجراء واحد بشكل مشترك)، أو إذا كان فريقك من ذوي الخبرة في المساعدات النقدية والقسائم والسياق، يمكنك إدارة ورشة عمل تحليل الاقتصاد السياسي مع تمثيل من مجموعة متنوعة من الجهات الفاعلة في المساعدات النقدية والقسائم لسحب وتقييم الموضوعات الرئيسية.

من الناحية المثالية، سيتم دمج تحليل الاقتصاد السياسي (أو التعلم منه) في تحليل وضع المساعدات النقدية والقسائم ودراسة ملاءمة المساعدات النقدية والقسائم والجدوى وتقييم المخاطر والفوائد والأضرار. يجب أن توجه صانعي القرار في مؤسستك بشأن القضايا المتعلقة بالبيانات لاعتبارها قبل توقيع عقد أو اتفاقية للمشاركة في الاستجابة (على سبيل المثال قرار "المتابعة – عدم المتابعة"). ستحتاج على الأرجح إلى القيام ببعض الدعوة الداخلية لمساعدة صانعي القرار على أن يصبحوا أكثر وعياً بالحاجة إلى أن يكونوا مستعدين للبيانات قبل الانخراط في المساعدات النقدية والقسائم

تحديد أي من سياسات خصوصية البيانات الوطنية وأطر العمل القانونية الأخرى سينطبق

تعمل البلدان في جميع أنحاء العالم بشكل متزايد على تطوير أو تحديث قوانين خصوصية البيانات للتكيف مع الحقائق الجديدة للمجتمعات الرقمية. يجب على الجهات الفاعلة في المساعدات النقدية والقسائم أن تكون على دراية بهذه الأمور وأن تحرص على متابعتها. قد تكون مراجعة أنظمة البيانات جزءًا من تقييمك التنظيمي المعتاد، وإذا لم يكن الأمر كذلك فقد ترغب في مراجعة المجالات أدناه. في حين أن آليات المساءلة لقوانين خصوصية البيانات قد تكون ضعيفة في بعض السياقات، فإن انتهاك قانون خصوصية البيانات قد يؤدي إلى تغريم المنظمة أو منعها من العمل.

13 مقتبس من المذكرة الإرشادية لبنك التنمية الآسيوي حول استخدام تحليل الاقتصاد السياسي لعمليات بنك التنمية الآسيوي 2009. راجع المنشور الكامل لمعرفة المزيد عن PEA. المصادر جيه مونكريف وسي لوتريل 2005. إطار تحليلي لفهم الاقتصاد السياسي للقطاعات وساحات السياسة. لندن: معهد التنمية لما وراء البحار؛ فريتز ك. كايزر وب. ليفي 2009. الحوكمة المدفوعة بالمشكلة وتحليل الاقتصاد السياسي: إطار الممارسة الجيدة. واشنطن العاصمة: البنك الدولي.

قد تكون الوكالات التي تتخذ من أوروبا مقراً لها ملزمة بالنظام الأوروبي العام لحماية البيانات والتي تعتبر بأنها توفر أعلى مستوى من حماية البيانات في العالم، حيث تتمتع وكالات مثل الأمم المتحدة واللجنة الدولية للصليب الأحمر ببعض الحماية القانونية التي تهدف إلى مساعدتها في الحفاظ على السرية والحياد في عملياتها.[14] في حين أن حصانتهم تعني أنهم غير ملزمين بالنظام الأوروبي العام لحماية البيانات، فإن لدى الأمم المتحدة واللجنة الدولية للصليب الأحمر سياسات حماية البيانات الخاصة بهما والتي يجب الالتزام بها.

قد يكون من المعقد إدارة العديد من الولايات القضائية القانونية في استجابة واحدة، حيث يمكن أن يساعدك العمل مع الفرق القانونية والتخطيط وتحديد أين تعبر البيانات الحدود وما هي المجموعات السكانية التي تتعلق بها على الامتثال لهذه القوانين ومجموعات القوانين. بعض السياقات مثل بنغلاديش والفلبين لديها متطلبات تتعارض مع النظام الأوروبي العام لحماية البيانات. بالإضافة إلى ذلك، تتطلب بعض الأنظمة إجراء تقييمات تأثير خصوصية البيانات إذا تم الوصول إلى حدود معينة تتعلق بنوع وكمية البيانات التي تم جمعها ومعالجتها ومستوى حساسية البيانات أو إذا تم جمع البيانات من السكان المعرضين للخطر. قد تتطلب أيضاً تقييمات تثبت أن جمع البيانات ومعالجتها لا يؤدي إلى ضرر أو انتهاك حقوق إضافية مثل حقوق الخصوصية.

تتضمن بعض التشريعات الوطنية اللوائح المتعلقة بنقل البيانات. قد يتم نقل البيانات داخل وبين المكاتب في البلد أو عبر البلدان. في جميع هذه الحالات توجد قواعد خاصة لحماية خصوصية وأمن البيانات الشخصية أو الحساسة التي يتم نقلها. عند حدوث عمليات نقل البيانات عبر الحدود، يُشار إلى ذلك باسم نقل البيانات عبر الحدود. بعض الدول لديها قوانين تهدف إلى تقييد عمليات نقل البيانات عبر الحدود، حيث قامت كينيا على سبيل المثال بسن قانون توطين البيانات الذي يقيد أنواع البيانات التي يمكن نقلها خارج البلاد. لدى الاتحاد الأوروبي أيضاً قواعد محددة تتعلق بمكان ووقت نقل بيانات مواطني الاتحاد الأوروبي خارج الاتحاد الأوروبي. تتطلب بعض البلدان تخزين نسخة من البيانات محلياً أو أن تتم معالجة البيانات في الدولة أو أن يتم الحصول على موافقة الحكومة قبل نقل البيانات. لدى المنظمات الدولية أيضاً قواعد حول متى وكيف يمكن أن يحدث النقل عبر الحدود.

في بعض الحالات قد تواجه المنظمات مخاطر مرتبطة بالاحتفاظ بالبيانات المخزنة في البلد، على سبيل المثال إذا كانت الحكومة تضطهد مجموعة معينة من الأفراد أو الجماعات وكان من الممكن استخدام البيانات التي تم جمعها من قبل السلطات لتحديد موقع تلك المجموعات، أو إذا تدهور الوضع الأمني إلى درجة أن المنظمة لا تشعر أنها قادرة على الحفاظ على البيانات آمنة ومحمية في الدولة. في هذه الحالات، تحتاج المؤسسات إلى اتخاذ قرارات صعبة بشأن اتباع القوانين مقابل تعريض الأشخاص للخطر وقد تقرر تجنب جمع البيانات في هذه الحالات.

الصندوق 8: الجوانب الرئيسية لمراجعتها فيما يتعلق بأنظمة أمن وخصوصية البيانات

- أنواع البيانات المشمولة في القوانين والسياسات
- القيود المفروضة على أنواع البيانات التي يمكن جمعها
- متطلبات فهم وتقييم المخاطر وتأثيرها على حقوق الأفراد
- قواعد محددة حول بيانات الأطفال أو بيانات الفئات الخاصة الأخرى مثل القياسات الحيوية
- المواصفات الخاصة بمشاركة البيانات
- المسؤوليات / المسؤوليات لمن يجمع البيانات مقابل أولئك الذين يعالجون البيانات
- القيود المفروضة على إمكانية نقل البيانات خارج الدولة
- قيود على مكان وكيفية تخزين البيانات أو إلى متى
- القواعد المتعلقة بما إذا كان يجب السماح للحكومات بالوصول إلى البيانات
- التوجيه حول كيفية جمع وتسجيل الموافقة
- الغرامات أو الإجراءات العقابية الأخرى التي يمكن تطبيقها على سوء التعامل مع البيانات
- حقوق "أصحاب البيانات" (أولئك الذين يتم جمع بياناتهم أو معالجتها)
- الآليات المطلوبة للتعامل مع الشكاوى
- مؤشرات حول متى وكيف ولمن يجب الإبلاغ عن انتهاكات البيانات
- متطلبات تعيين مسؤول حماية البيانات

14 تشمل الامتيازات والحصانات التي تتمتع بها اللجنة الدولية للصليب الأحمر ووكالات الأمم المتحدة الحصانة من الإجراءات القانونية، كما أن مبانيها ووثائقها وبياناتها محمية أيضًا من الوصول إليها من قبل الحكومات في المناطق التي تعمل فيها. يُعفى موظفوها من الإدلاء بالشهادة أو تقديم الأدلة في الإجراءات القانونية. انظر اتفاقية امتيازات وحصانات الأمم المتحدة (1946) على سبيل المثال واقرأ المزيد عن الوضع القانوني للجنة الدولية للصليب الأحمر.

بالإضافة إلى قوانين الخصوصية، فإن التشريعات الوطنية المنبثقة عن فريق عمل الإجراءات المالية أو قواعد العناية الواجبة[15] للمستهلك مثل متطلبات اعرف عميلك قد تفرض عليك جمع معلومات معينة من أجل إجراء التحويلات النقدية (انظر الوثيقة الإرشادية 3 لمعرفة المزيد عن متطلبات فريق عمل الإجراءات المالية واعرف عميلك).

اعمل مع فرق الشؤون القانونية والخصوصية وتكنولوجيا المعلومات لديك للعثور على خيارات نقل البيانات وتخزينها. راجع مكان وكيفية قيام الأطراف الخارجية التي تعمل معها بنقل البيانات وتخزينها.

منشور ITIF **تدفقات البيانات عبر الحدود: أين العوائق وماذا تكلف؟** يوفر قائمة (منذ 2017) بالبلدان التي لديها سياسات أو قوانين تعريب البيانات. يمكنك أيضاً التحقق من **قوانين حماية البيانات العالمية** الخاصة بشركة DLA Piper (المحدثة باستمرار) أو منشور Deloitte (2017) **الخصوصية هي الأهم: حماية البيانات الشخصية في إفريقيا**.

قد تحتاج إلى الموازنة بين الخيارات الصعبة والمفاضلات، على سبيل المثال إذا كنت مطالبًا قانونياً بمشاركة البيانات مع الحكومات وتخشى أن يؤدي ذلك إلى تعريض السكان المتضررين للخطر أو التأثير على مستويات ثقتهم في مؤسستك. راجع "مشاركة البيانات مع الحكومات" **الصادرة عن شراكة التعلم النقدي**.

متطلبات امتثال المنحة ونظام وبيانات الجهة المانحة للبحث

تطلب الجهات المانحة بشكل متزايد من الجهات الفاعلة في المساعدات النقدية والقسائم تنسيق البيانات ومشاركتها. قد يكون لدى المانحين أيضاً متطلبات محددة بشأن أنواع البيانات التي يجب على الوكالات جمعها ومشاركتها أو كيف يتوقعون حماية البيانات، حيث سيتم تحديدها عادةً في مستندات اتفاقية المنحة وستؤثر على كيفية إدارة بيانات المساعدات النقدية والقسائم الخاصة بك وتخزينها. تتطلب بعض الجهات المانحة الحكومية على سبيل المثال فحص المستفيدين من المساعدات النقدية والقسائم أو الامتثال لتدابير مكافحة الإرهاب أو لوائح مكافحة غسل الأموال والمتطلبات التي يمكن أن تعرض مستلمي المساعدات النقدية والقسائم الفرديين للخطر نظراً لكمية البيانات الشخصية والحساسة التي يتم جمعها لإجراء عمليات الفحص هذه وعدم الوضوح بشأن من يمكنه الوصول إلى هذه الأنواع من قواعد البيانات واحتمالية حدوث أخطاء في التضمين أو الاستبعاد. يطلب البعض الآخر مشاركة بيانات برمجية معينة معهم في تنسيقات وأطر زمنية محددة وستحتاج المؤسسات إلى إخفاء هوية البيانات أو معالجتها بطريقة أخرى قبل مشاركتها حتى يتم حماية بيانات متلقي المساعدات النقدية والقسائم. قد يكون البحث عن متطلبات بيانات المانحين جزءاً من تقييمات الجدوى الخاصة بك؛ ومع ذلك في بعض الأحيان لا تبحث المؤسسات عن كثب بشكل كافٍ في المتطلبات المتعلقة بالبيانات على وجه التحديد.

بالإضافة إلى ذلك، بالنسبة لبعض المنح أو الشراكات يُتوقع من الشركاء إدخال البيانات في أنظمة محددة للأمم المتحدة،مثل SCOPE التابع لبرنامج الغذاء العالمي[16] و PRIME/ProGres التابع لمفوضية الأمم المتحدة لشؤون اللاجئين [17] و / أو برنامج Primero التابع لليونيسف[18]. في حالات أخرى، سيتم مشاركة البيانات بشكل ثنائي الجانب بين الجهات الفاعلة في المنظمات غير الحكومية من خلال تفويضات الاتحادات وهيكليات الحوكمة واتفاقيات مشاركة البيانات. في كثير من الأحيان، يتم إنشاء أنظمة الأمم المتحدة لجمع البيانات البيومترية، وقد كانت مشاركة البيانات واستخدام هذه الأنظمة بمثابة مجال توتر بين وكالات الأمم المتحدة وبعض الشركاء المنفذين الذين لديهم مخاوف بشأن حماية البيانات وقوة أمن بعض منصات البيانات. لقد أعربت بعض المنظمات غير الحكومية عن إحباطها من اختلال موازين القوى ومساحة التفاوض بشأن متطلبات الأمم المتحدة ، فضلاً عن امتيازات وحصانات الأمم المتحدة. يعتبر موضوع مشاركة البيانات واستخدامها لأنظمة البيانات هذه هو موضوع التدفق المستمر على خلفية المحادثات والمفاوضات الجارية، حيث يعمل برنامج الأغذية العالمي ومفوضية الأمم المتحدة لشؤون اللاجئين واليونيسيف حالياً على طرق لجعل أنظمتها قابلة للعمل المتبادل مع بعضها البعض ومع الحكومات مما أثار مخاوف بشأن مسؤولية البيانات بين الشركاء المنفذين.

من المهم في مرحلة ما قبل العرض أن تفهم متطلبات المانحين وما إذا كانت تتوافق مع ماهية مؤسستك وما لا ترغب في القيام به. من خلال إجراء البحث قبل تطوير الاقتراح، يمكنك أن تقرر ما إذا كنت تريد المتابعة و / أو كيفية التفاوض بشأن متطلبات بيانات المانحين.

أعرب العديد من المانحين عن استعدادهم لتغيير متطلبات البيانات إذا أثيرت مخاوف مشروعة. من خلال إجراء البحث الخاص بك ثم صياغة أو توثيق أي مخاوف. من خلال بحثك وصياغة أو توثيق أية مشكلات، سيكون لديك حجة أقوى للتواصل مع المتبرع للتفاوض.

قد تواجه معارضة من أجزاء أخرى من مؤسستك لديها وعي أقل بالمخاطر التي يمكن أن تشكلها البيانات أثناء التنفيذ. من المهم بناء تحالفات داخل مؤسستك للدعوة إلى حماية أكبر للبيانات وإدارة مسؤولة للبيانات ولإيجاد طرق لإشراك الفرق المتحالفة مثل الحماية والقانونية وتكنولوجيا المعلومات والأمن السيبراني لبناء المزيد من الدعم لمسؤولية البيانات.

15 انظر مجموعة العمل المالي (2020) "المعايير الدولية لمكافحة غسل الأموال وتمويل الإرهاب وانتشار الأسلحة: توصيات مجموعة العمل المالي
16 انظر نبذة عامة عن سياق برنامج الأغذية العالمي
17 انظر توجيهات وكالة الأمم المتحدة للاجئين حول التسجيل وإدارة الهوية 3.6 النظام البيئي لتسجيل السكان وإدارة الهوية (برايمز)
18 انظر موقع اليونيسف بريميرو

استعراض قدرة إدارة البيانات المؤسسية

تعتمد الاستجابات الإنسانية بما في ذلك المساعدات النقدية والقسائم على جهات فاعلة متعددة وتعتبر حماية البيانات آمنة فقط كحلقة أضعف. تزداد أهمية تعزيز سياسة وممارسات حماية البيانات مع تزايد رقمنة المنظمات والاستجابات وتجميع كميات أكبر من البيانات الحساسة ومشاركتها.

سيكون للمنظمات مستويات مختلفة من القدرة على إدارة البيانات، إذ لا يعتمد هذا على حجم المنظمة بل على الأهمية التي أولتها إلى هذا المجال وحصولها على التمويل المؤسسي بمرور الوقت لتحسين البنية التحتية للبيانات والأنظمة. **من الأهمية بمكان ألا تقوم المؤسسات بجمع البيانات التي لا يمكنها الاحتفاظ بها بأمان، وهذا هو المفهوم الأساسي لمسؤولية البيانات.**

يمكن أن تساعدك المراجعة التنظيمية على تحديد ما إذا كانت مؤسستك وشركاؤك المحتملين لديهم القدرة على إدارة البيانات بمسؤولية في السياق الذي تعمل فيه، ويجب أن يتم ذلك قبل وجود مشاركة أو التزام رسمي لتقديم المساعدات النقدية والقسائم في سياق معين.

يمكنك إجراء تقييم شامل لأهلية بياناتك (أو بيانات منظماتك الشريكة) باستخدام **نموذج أهلية البيانات المسؤول للتنمية والمنظمات الإنسانية** الذي تم تطويره من أجل منظمة كير. تتطلب المراجعة المؤسسية الواسعة وخطة التعزيز وقتًا واستثماراً طويل الأجل.

إذا لم تكن مؤسستك قادرة على إجراء تقييم كامل أو منفصل فيمكنك تضمين قسم حول قدرة مسؤولية البيانات في تقييم جدوى المساعدات النقدية والقسائم العام الخاص بك. يمكن أن يساعد النموذج الموجود في الصندوق 9 أدناه في تحديد الأسئلة الأساسية التي يجب تضمينها.

يمكن أن تساعدك **قائمة المراجعة القابلة للطباعة هذه من Electronic Frontier Foundation** في تقييم أمان البيانات وقدرة الخصوصية لشريك معالجة البيانات، وقد تساعدك أيضاً في تقييم جهة خارجية أو مقدم خدمات رعاية صحية.

تعمل **مجموعة الأسئلة** هذه كدليل للاستعلام عن امتثال جهة خارجية أو امتثال البائع للنظام الأوروبي العام لحماية البيانات.

اتخاذ القرار بشأن المتابعة من عدم المتابعة

بناءً على الأبحاث والتقييمات المذكورة أعلاه والتي تهدف إلى فهم أفضل لسياقك وقدراتك؛ حدد على مستوى عالٍ ما إذا كنت ستنتقل إلى مرحلة الاقتراح أو الشراكة وما إذا كنت تريد المشاركة في استجابة معينة.

كما لوحظ، إذا كانت مؤسستك تقوم بالفعل بإجراء تقييمات الجدوى أو القدرات أو المخاطر فيمكن دمج الجوانب المذكورة أعلاه في تلك. من المهم أن يتم تقييم مسؤولية البيانات على وجه التحديد حتى تكون متأكدًا من أخذها في الاعتبار في عملية صنع القرار. قد يكون هذا مجالاً جديداً لاعتبار منظمتك وقد يتطلب تأييدًا مع صانعي القرار من أجل مناقشته في مرحلة ما قبل الاقتراح. **من المهم ملاحظة أن بعض المشاريع قد تحتاج إلى التوقف فعليًا بعد مرحلة التحليل الأولية هذه أو إيجاد طرائق لا تجمع البيانات الحساسة لأن القدرة على جمعها بأمان غير موجودة في المنظمة أو الاستجابة.**

إذا لم يكن لدى مؤسستك نموذجاً أو عملية لتحديد ما إذا كان سيتم المضي قدماً أم لا بناءً على سياق البيانات والقدرة، يمكنك استخدام النموذج في الصندوق 9 أدناه. عند تعبئة النموذج، رتب مكانك الحالي وقدم توصيات لإجراءات التخفيف التي يمكن أن تغير قرار عدم المتابعة إلى قرار متابعة. إذا كانت لديك عملية قائمة فيمكن دمج الأسئلة أدناه فيها حتى تكون متأكداً من أنك تغطي البيانات المسؤولة في تقييماتك المبكرة.

الصندوق 9: تقييم سريع للمتابعة أو عدم المتابعة

إذا لم يكن لدى مؤسستك عمليات قائمة أو كنت بحاجة إلى نموذج تقييم سريع، فقد تساعدك أداة المتابعة من عدم المتابعة هذه. استخدمها لتقييم مدى ثقتك في أن مؤسستك يمكنها إدارة البيانات بمسؤولية في سياق هذه الاستجابة.
بعد ذلك قدم الملاحظات في الصناديق حول سبب ثقتك أو عدم ثقتك بنفسك واقترح أي استراتيجيات يجب اتخاذها لتحسين الثقة، مثل تقييم المهارات والقدرات والموارد. استخدم الإجابات كجزء من قرارات المتابعة – عدم المتابعة أو شاركها مع أولئك الذين يتفاوضون بشأن المشاركة في المنحة. يجب أن تحاول الحصول على مدخلات من مجموعة متنوعة بما في ذلك الشؤون القانونية والحماية وتكنولوجيا المعلومات والأمن السيبراني والبيانات أو المراقبة والتقييم والمساءلة والتعلم وموظفي الخطوط الأمامية. يجب على مسؤول لجنة حماية البيانات والأخلاقيات (أو أي وظيفة أخرى مماثلة) مراجعة هذا النموذج ودعم عملية صنع القرار، ويمكن أيضاً استخدام هذا النموذج لتقييم مستويات ثقتك في شركائك.

مستويات الثقة (المهارات، القدرة، الموارد)	منخفض	متوسط	مرتفع
نحن نعلم كيف سيتم استخدام البيانات وقد حددنا جميع الأطراف التي ستتمكن من الوصول إلى البيانات			
لقد قمنا بتقييم جدوى العمل في هذا السياق دون وضع متلقي المساعدات النقدية والقسائم أو مؤسستنا أو موظفينا في مستويات غير مقبولة من مخاطر الضرر من البيانات			
يمكننا الامتثال للأطر القانونية الوطنية والعالمية			
يمكننا الحفاظ على أمان البيانات أثناء اتباع الأطر القانونية الوطنية والعالمية			
يمكننا الامتثال لمتطلبات حماية بيانات الجهات المانحة			
يمكننا الحفاظ على أمان البيانات أثناء تزويد المتبرعين بالبيانات التي يحتاجون إليها			
يمكننا الحفاظ على أمان البيانات في الأنظمة التي يطلب منا المانحون أو الشركاء استخدامها			
لدينا القدرة على إدارة الأنظمة المطلوب منا استخدامها			
لدينا القدرة الكلية لإدارة البيانات بمسؤولية في هذا السياق			
يتمتع شركاؤنا بالقدرة على إدارة البيانات بمسؤولية في هذا السياق			

2 الوثيقة الإرشادية

التصميم والتخطيط

بمجرد أن يكون هناك قرار رفيع المستوى بشأن ما إذا كان سياق العمل والقدرات المؤسسية والشروط المتعلقة بالبيانات تسمح باستجابة المساعدات النقدية والقسائم المسؤولة (بحسب الوثيقة الإرشادية 1)، يجب تصميم خطة جمع البيانات وإدارتها للاستجابة الشاملة. ستدخل تقييمات السياق والقدرات في الوثيقة الإرشادية 1 في هذه المرحلة، حيث ستصمم مقترح المساعدات النقدية والقسائم الخاص بك وتوضح كيف ستتم إدارة البيانات خلال الاستجابة (ستساعدك الوثائق الإرشادية 3-7 على تطوير تفاصيل كل مرحلة من مراحل دورة حياة البيانات). في هذه المرحلة قد تقوم أيضاً بإجراء تقييمات الجدوى النقدية وإجراء مراجعة مؤسسية إضافية وإجراء تقييم للسوق وتقييم مزودي الخدمة المالية وتقييمات الاحتياجات ونقاط الضعف واتخاذ القرارات بشأن طرق المساعدات النقدية والقسائم الأنسب والأكثر أماناً للسياق.[19]

ستقوم بتحديد الشركاء والأطراف الثالثة الأخرى التي ستعمل معها والأنظمة التي ستستخدمها والشكل الذي ستبدو عليه العملية الشاملة وما إذا كان من الممكن ربط المساعدات النقدية والقسائم الإنسانية بأنظمة الحماية الاجتماعية الحكومية. في كل هذه الجهود سترغب في تقييم مسؤولية البيانات، وفي الوقت نفسه يجب أن تغذي العوامل المختلفة المتعلقة بمسؤولية البيانات القرارات المتعلقة بكيفية تصميم البرنامج وتنفيذه وما إذا كان من الآمن جمع أنواع معينة من البيانات أو ما إذا كانت المخاطر المتعلقة بالبيانات عالية جدًا بالنسبة للسكان المتأثرين أو العاملين في الخطوط الأمامية ومسؤول التعداد أو لمنظمتك بشكل عام.

أثناء مرحلة التصميم والتخطيط ستضع كل عملية من عمليات البيانات التي ستحدث خلال الاستجابة بأكملها - بدءاً من تقييمات الاحتياجات ومروراً بالاستهداف والتسجيل والمشاركة والتسليم ولغاية المراقبة والتقييم والمساءلة والتعلم والتغذية الراجعة من السكان المتأثرين - وكيف ستقوم بإدارة البيانات بمسؤولية. سيسمح لك التصميم والتخطيط للبيانات المسؤولة بفهم الشكل الذي قد تبدو عليه استجابتك من خلال نهج بيانات مسؤول وناضج تماماً للتكيف مع الوقت والتمويل المتاحين لديك ولتحديد المجالات التي تحتاج إلى تحسين بمرور الوقت. مع تطور القدرات والممارسات من الناحية النموذجية ستصبح مسؤولية البيانات بمثابة عقلية وليست عبئاً.

تغطي الوثيقة الإرشادية 2 التصميم والتخطيط، حيث ستكون قد أنجزت عمل الصورة الكبيرة في الوثيقة الإرشادية 1 وستحتاج الآن إلى الخوض في مزيد من التفاصيل حول الشكل الذي ستبدو عليه استجابتك في الممارسة العملية. سيغذي ذلك تصميم الاقتراح والميزانية واختيار الشريك وقرارات التخطيط الأخرى.

19 راجع "سياسة الحد الأدنى للمعايير النقدية" من ميرسي كوربس للحصول على نبذة عامة عن التقييمات والمعايير المختلفة التي تدمجها المنظمة في كل مرحلة من مراحل استجابة المساعدات النقدية والقسائم

حدد ما إذا كنت ستستخدم البيانات القائمة أو ستجمع بيانات جديدة

كجزء من عملية التصميم والتخطيط ستحتاج إلى تحديد ما إذا كنت بحاجة إلى إجراء عملية جديدة تمامًا لجمع البيانات أو ما إذا كانت هناك قوائم أو مجموعات بيانات قائمة يمكن استخدامها للاستهداف أو المشاركة أو التسليم. إذا كانت هذه القوائم قديمة أو منخفضة الجودة أو إذا تم تغييرها بطريقة غير مصرح بها أو كانت تغطي جزءاً معيناً فقط من السكان فسيلزم استكمالها ببيانات إضافية أو عملية جديدة لجمع البيانات. يمكن أن يمثل تكرار البيانات بين القوائم الجديدة والقوائم القائمة مشكلة، وفي هذه الحالة ستحتاج إلى مقارنة القوائم وتقييم الموقف. إذا لم تكن الأنظمة قابلة للتشغيل فقد يمثل ذلك تحدياً. في بعض الاستجابات قد تكون إحدى المنظمات أو الوكالات قد قارنت بالفعل القوائم والبيانات وامتثلت لها، ومع ذلك قد يكون من الجيد الدعوة إلى تحديث البيانات أو مراجعتها من أجل الجودة أو أكثر شمولاً.

إذا كانت استجابتك مرتبطة بمبادرة حماية اجتماعية قائمة فستكون هناك حاجة إلى تنسيق البيانات الإنسانية مع البيانات الحكومية، حيث يثير هذا مخاوف بشأن وصول الحكومة إلى القوائم الإنسانية. على سبيل المثال قد تؤدي قوائم السكان النازحين داخلياً واللاجئين والمهاجرين إلى خطر الاستهداف أو الاحتجاز أو الترحيل أو أنواع أخرى من الانتهاكات من قبل الحكومات. إذا كنت تخطط لاستخدام البيانات القائمة فسيكون من المهم أن تقوم بمراجعة الجوانب القانونية للوصول إلى البيانات التي تم جمعها واستخدامها لغرض واحد لتحقيق غرض آخر. (انظر الوثيقة الإرشادية 2 والصناديق 12 و 13 بشأن الأسس القانونية لمعالجة البيانات).

لقد دفعت جائحة كوفيد-19 العديد من الوكالات إلى استخدام مجموعات البيانات القائمة والابتكار عبر المساعدات النقدية والقسائم والحماية الاجتماعية الإنسانية. بعض هذه الابتكارات مذكورة في SocialProtection.org وفي **منشور المدونة** هذا على وجه الخصوص.

تقدم ميرسي كوربس **إرشادات حول أنواع مختلفة من البيانات التي يمكن استخدامها أو إعادة استخدامها للاستهداف** عن بُعد جنبًا إلى جنب مع **إيجابيات وسلبيات** كل مصدر.

اطلع على دراسة حالة شراكة التعلم النقدي حول **الأساليب الناشئة لاستخدام البيانات غير التقليدية لاستهداف المساعدات النقدية والقسائم**.

وثق GovLab كيف أجروا **"جمع البيانات"** لفهم الحالات التي يكون فيها سكان مدينة نيويورك مرتاحين للوصول إلى بياناتهم وإعادة استخدامها أثناء أزمة كوفيد-19، ويمكن استخدام هذه المنهجية في سياقات أخرى أيضاً.

قرر من سيعمل كمراقب للبيانات ومعالج للبيانات

في بداية استجابة المساعدات النقدية والقسائم سيكون من الضروري فهم من سيعمل كمراقب للبيانات ومن سيعمل كمعالج بيانات أو ما إذا كان سيكون هناك مراقبون مشتركون للبيانات. مراقب البيانات هو الكيان الذي يتخذ قرارات حول كيفية معالجة البيانات الشخصية. يتلقى المعالج تعليمات من وحدة التحكم بشأن البيانات الشخصية التي يتم جمعها وكيفية معالجتها. عندما تعمل المنظمات كوحدات تحكم مشتركة فإنها تقرر معاً أغراض ووسائل معالجة البيانات الشخصية ذاتها.

الصندوق 10: أدوار ومسؤوليات مراقبي ومعالجي البيانات

تعتمد التزامات المؤسسة فيما يتعلق بالبيانات على الدور الذي تلعبه في جمع البيانات ومعالجتها. بموجب النظام الأوروبي العام لحماية البيانات يمكن للأفراد والسلطات الإشرافية على سبيل المثال محاسبة كل من وحدات المراقبة والمعالجين على عدم امتثالهم لمسؤولياتهم بموجب النظام.

مراقب البيانات: هو الكيان الذي يمارس بمفرده أو بالاشتراك مع آخرين مراقبة أغراض ووسائل معالجة البيانات الشخصية هو مراقب البيانات. يتحمل المراقبون أعلى مستوى من مسؤولية الامتثال للبيانات. يجب عليهم إثبات الامتثال لمبادئ حماية البيانات ومتطلبات القانون العام لحماية البيانات الأخرى، وهم أيضا مسؤولون عن امتثال معالج (معالجي) البيانات الخاصة بهم. يمكن للسلطات الإشرافية والأفراد اتخاذ إجراءات ضد مراقب فيما يتعلق بخرق التزاماته. مراقبو البيانات هم أولئك الذين:

- يقرروا جمع البيانات الشخصية أو معالجتها
- يحددوا الغرض أو النتيجة من المعالجة
- يحددوا البيانات الشخصية التي يجب جمعها
- يحددوا الأفراد المطلوب جمع بيانات شخصية عنهم
- يحصلوا على مكاسب تجارية أو فائدة أخرى من المعالجة باستثناء أي مدفوعات مقابل خدمات من وحدة مراقبة أخرى

الصندوق 10: أدوار ومسؤوليات مراقبي ومعالجي البيانات

- يعالجوا البيانات الشخصية نتيجة لعقد بيننا وبين صاحب البيانات
- يتخذوا قرارات بشأن الأفراد المعنيين كجزء من المعالجة أو كنتيجة لها
- يمارسوا الحكم المهني في معالجة البيانات الشخصية
- لهم علاقة مباشرة بموضوعات البيانات
- يتمتعوا باستقلالية كاملة فيما يتعلق بكيفية معالجة البيانات الشخصية
- قاموا بتعيين المعالجين لمعالجة البيانات الشخصية نيابة عنهم

المراقب المشترك: إذا حدد اثنان أو أكثر من مراقبي البيانات معاً أغراض ووسائل معالجة البيانات الشخصية ذاتها، فإنهم يعتبرون وحدات مراقبة مشتركة. ومع ذلك فهي ليست وحدات مراقبة مشتركة إذا كانت تقوم بمعالجة نفس البيانات لأغراض مختلفة. يجب أن يرتب المراقبون المشتركون فيما بينهم من سيتحمل المسؤولية الأساسية عن الامتثال لالتزامات النظام الأوروبي العام لحماية البيانات ولا سيما التزامات الشفافية وحقوق الأفراد. تظل جميع وحدات المراقبة المشتركة مسؤولة عن الامتثال لالتزامات وحدة المراقبة بموجب النظام الأوروبي العام لحماية البيانات. يجوز لكل من السلطات الإشرافية والأفراد اتخاذ إجراءات ضد أي مراقب فيما يتعلق بخرق تلك الالتزامات. تعتبر المنظمات وحدات مراقبة مشتركة في الحالات التي تكون فيها:

- لديها هدف مشترك مع الآخرين فيما يتعلق بالمعالجة
- تقوم بمعالجة البيانات الشخصية لنفس الغرض مثل وحدة مراقبة أخرى
- تستخدم نفس مجموعة البيانات الشخصية (مثل قاعدة بيانات واحدة) لهذه المعالجة كمراقب آخر
- صممت هذه العملية مع وحدة مراقبة أخرى
- لديها قواعد مشتركة لإدارة المعلومات مع وحدة مراقبة أخرى

معالج البيانات: الكيان الذي يعالج البيانات الشخصية نيابة عن أو بموجب تعليمات مراقب البيانات هو معالج البيانات. ليس لدى معالجي البيانات أي غرض خاص بهم لمعالجة البيانات، ولا تتحمل المعالجات نفس التزامات وحدات المراقبة بموجب النظام الأوروبي العام لحماية البيانات ولا يتعين عليها دفع رسوم حماية البيانات. ومع ذلك فإن المعالجات لديها التزامات مباشرة خاصة بها بموجب النظام الأوروبي العام لحماية البيانات. يجوز لكل من السلطات الإشرافية والأفراد اتخاذ إجراءات ضد المعالج فيما يتعلق بخرق تلك الالتزامات. معالجي البيانات هم أولئك الذين:

- يتبعوا التعليمات من شخص آخر فيما يتعلق بمعالجة البيانات الشخصية
- يتم إعطاؤهم البيانات الشخصية من قبل عميل أو طرف ثالث مشابه أو تم إخبارهم بالبيانات التي يجب جمعها
- لا يتخذوا قراراً بجمع البيانات الشخصية من الأفراد
- لا يقرروا ما هي البيانات الشخصية التي ينبغي جمعها من الأفراد
- لا يقرروا الأساس القانوني لاستخدام تلك البيانات
- لا يقرروا الغرض (الأغراض) التي سيتم استخدام البيانات من أجلها
- لا يقرروا الإفصاح عن البيانات أو لمن
- لا يقرروا كم من الوقت للاحتفاظ بالبيانات
- يتخذوا بعض القرارات بشأن كيفية معالجة البيانات ولكن يقوموا بتنفيذ هذه القرارات بموجب عقد مع شخص آخر
- غير مهتمين بالنتيجة النهائية للمعالجة

(المفاهيم وقوائم التحقق مستخلصة من مكتب مفوض المعلومات الخاص بالمملكة المتحدة ومعدلة بأقل مدىً ممكن).[20]

سيكون تحديد الأدوار (وحدة المراقبة والمعالج) مهماً للجوانب اللاحقة مثل اتفاقيات مشاركة البيانات وبروتوكولات نقل المعلومات. من المهم أيضاً مع بدء الاستجابة أن يتضح من هو المسؤول وعرضة للمساءلة عن أي جوانب معالجة البيانات، كما ستحتاج أيضاً إلى هذه المعلومات لإعلام الأفراد والمجتمعات بكيفية التعامل مع بياناتهم.

انظر التفسير التفصيلي لمسؤوليات مراقبي ومعالجي البيانات بموجب النظام الأوروبي العام لحماية البيانات.

20 Information Commissioner's Office of the UK (2018) 'Guide to the General Data Protection Regulation: Controllers and Processors'.

الصندوق 11: مراقبة البيانات الشائعة – سيناريوهات معالجة البيانات

لتحديد من هو مراقب البيانات ومن هو معالج البيانات، ستحتاج إلى الإجابة على السؤال "من يتخذ القرارات بشأن الأنظمة المستخدمة وأي البيانات يتم جمعها؟". نوضح أدناه بعض السيناريوهات المحتملة لوحدة المراقبة – المعالج.

إذا تم إشراك جهة مانحة أو كيان تابع للأمم المتحدة وشركاء منفذين، فقد ترى أحد هذه السيناريوهات:

- جهة مانحة / وكالة تابعة للأمم المتحدة أو تمويل يتم توفيره ذاتيًا – حيث يكون الشريك المنفذ كمراقب
- جهة مانحة إلزامية أو كيان تابع للأمم المتحدة يطلب أنظمة / مناهج / بيانات محددة – يكون المانح كمراقب والشريك المنفذ (المستفيد) كمعالج

إلى حد ما قد يكون هذا قراراً سياسياً، حيث قد يرغب الشركاء المنفذون الذين يشعرون بأنهم أصحاب مبادئ أكثر من المانحين / وكالة الأمم المتحدة في العمل كمراقب هنا أو إذا كانوا يريدون تقليل المسؤولية فقد يرغبون في أن يعمل المانح / وكالة الأمم المتحدة كمراقب.

بين المنظمات غير الحكومية والمنظمات غير الحكومية الدولية:

قد يكون هذا بسيطاً جدًا أو قد يكون أكثر تعقيدًا إذا كانت المنظمة غير الحكومية أو المنظمات غير الحكومية الدولية تعمل بالشراكة مع آخرين - على سبيل المثال برنامج متعلق بالائتلاف. تتضمن بعض السيناريوهات ما يلي:

- تعمل المنظمات غير الحكومية أو المنظمات غير الحكومية الدولية إلى حد كبير بمفردها مع موظفيها الميدانيين وبرمجة "الحلقة المغلقة" الورقية / الرقمية. في هذه الحالة ينتهي خط الأنابيب هنا
- في ائتلاف مسطح للغاية حيث لا يمكن تمييز الأدوار تقريباً، قد ترى مراقبي البيانات المشتركين، ومع ذلك قد تكون الفرق القانونية غير مرتاحة لهذا بسبب مقدار المسؤولية التي يفرضها لأنه يمكنك استخدام أي من أعضاء وحدة المراقبة في البيانات المشتركة لخرق أي بيانات أخرى. قد تجد فرق الخصوصية والفرق الميدانية صعوبة في التواصل مع بعضها البعض في هذه الحالة لأن لديهم حتماً رغبات مختلفة جدًا في المخاطرة
- عندما يكون لدى عضو الائتلاف "قائد" واضح فقد يكون مراقباً أو معالجاً رئيسيًا ويصدر منحًا فرعية لشركاء آخرين؛ وفي هذا الإعداد يتحمل العميل المتوقع معظم مخاطر المسؤولية في حالة حدوث خرق للبيانات
- عندما يكون للائتلاف أدوار منفصلة تماماً (على سبيل المثال؛ يقوم العضو أ بتقديم الأمن الغذائي والعضو ب يقدم المشورة القانونية) فقد يكونون مراقبين منفصلين ("مراقبون مشتركون") ولديهم ببساطة اتفاقيات مشاركة البيانات ("لتجنب الشك")

شمول مقدمي الخدمة المالية:

عند مشاركة مقدمي الخدمات المالية من المحتمل أن يكون هناك احتمالان:

- لدى مقدم الخدمات المالية التزاماته الخاصة (على سبيل المثال "اعرف عميلك" أو يبيع أيضاً خدمات المستهلك إلى المستفيدين عبر بطاقات الحلقة المفتوحة) - وفي هذه الحالة قد يكونون مراقبًا منفصلاً - في هذه الحالة كما هو الحال مع "الأدوار المنفصلة" يمكن أن يكون هذا مع اتفاقية مشاركة البيانات لتجنب الشك / المراقب المشترك. في هذه الحالة سيكون من المثالي إجراء تقييم للمخاطر لتحديد الالتزامات المحتملة واستراتيجيات التخفيف من المخاطر التي يمكن تقديمها من خلال إشراك أو تأييد مقدم الخدمات المالية
- التزامات مقدم الخدمة المالية قليلة / لا توجد التزامات أخرى (نادرة ولكنها ممكنة. يمكن أن يندرج مقدم الخدمة مثل بائع برامج / أجهزة المساعدات النقدية والقسائم أيضاً ضمن هذه الفئة) - حيث قد يكون مقدم الخدمة المالية مجرد معالج. قد يكون أيضاً معالجاً لبعض الأنشطة ولكنه مراقب لأنشطة أخرى (على سبيل المثال قد يكون لدى العملاء بالفعل بطاقات خصم يكون البنك مراقباً لها، ولكنهم في بعض الأنشطة يعملون كمعالج لمنظمة غير حكومية دولية).

تحديد أساس قانوني لمعالجة البيانات قبل جمع البيانات الشخصية أو الحساسية

من أجل معالجة البيانات الشخصية أو الحساسة ستحتاج إلى تحديد أساس قانوني. قد يكون من المفيد التفكير في الأساس القانوني لجمع البيانات كبوابة أخلاقية وقانونية رئيسية لنشاط البيانات الإجمالي - تقريباً اختبار للمنفعة الاجتماعية والذي إذا فشل يشير إلى أن استخداماً معيناً للبيانات قد لا يكون لأفضل مصالح المجتمع أو الأفراد المتأثرين. تميل القواعد القانونية في القوانين الوطنية إلى التركيز على التوازن بين حقوق الأفراد والجماعات و "موقع الوكالة" - بعبارة أخرى؛ المكان الذي توجد فيه المراقبة والقوة والتكليف.

في بعض السياقات؛ يكون الأساس القانوني بسيطًا للغاية ويركز بالكامل على الاختيار الفردي. ومع ذلك فإن الأساس القانوني في القانون الأوروبي والسياقات المماثلة أكثر دقة ويقدم مسارات مختلفة تدرك أنه في بعض الأحيان يكون الاختيار غير ممكن، على سبيل المثال عندما تكون هناك حاجة عامة مهيمنة أو شرط لإنقاذ الحياة أو سبب آخر يجعل من الضروري جمع ومعالجة البيانات. عندما لا يكون الاختيار ممكنًا فغالبًا ما تكون هناك متطلبات متابعة إضافية يجب أن يفي بها أولئك الذين يرغبون في جمع البيانات ومعالجتها لضمان عدم انتهاك الحقوق الأخرى.

لهذه الأسباب؛ فإن الاختيار الصحيح للأساس القانوني ليس فقط ضمانًا قانونيًا مهماً بل هو مبدأ أساسي للتعرف وفهم أين تكمن القوة وتحديد جذر نشاطك في الغرض الاجتماعي.

الصندوق 12: الأسس القانونية لمعالجة البيانات

على سبيل المثال يدرج النظام الأوروبي العام لحماية البيانات القواعد القانونية الستة لمعالجة البيانات على النحو التالي:

- **الاهتمامات الحيوية:** المعالجة لازمة لحماية حياة شخص ما في حالات الطوارئ
- **المهمة / المصلحة العامة:** المعالجة لازمة لك لأداء مهمة للمصلحة العامة أو لوظائفك الرسمية والمهمة أو الوظيفة لها أساس واضح في القانون
- **الموافقة الفردية:** لقد أعطى الفرد موافقة واضحة لك لمعالجة بياناته الشخصية لغرض معين
- **المصالح المشروعة:** المعالجة لازمة لمصالحك المشروعة أو المصالح المشروعة لطرف ثالث ما لم يكن هناك سبب وجيه لحماية البيانات الشخصية للفرد والتي تتجاوز تلك المصالح المشروعة.
- **أداء العقد:** المعالجة لزمة للعقد الذي أبرمته مع الفرد أو لأنهم طلبوا منك اتخاذ خطوات محددة قبل إبرام العقد
- **الالتزام القانوني:** المعالجة لازمة لك للامتثال للقانون (لا يشمل الالتزامات التعاقدية)

تستخدم اللجنة الدولية نفس هذه الأسس القانونية الأساسية لجمع البيانات الشخصية ولكنها تجمع بين التعاقدية والقانونية في فئة واحدة. يجب تحديد الأساس القانوني قبل جمع البيانات ولا يمكن تبديل الأساس القانوني والغرض من جمع البيانات جزئياً من خلال أنشطة جمع البيانات ومعالجتها. في حالة حدوث ذلك؛ يجب إعادة جمع البيانات التي تم جمعها بالفعل ومعالجتها وفقًا للأساس القانوني المحدث.[21]

لقد كان هناك نقاش مكثف في القطاع الإنساني حول الأسس القانونية، لا سيما فيما يتعلق بوقت وما إذا كان يجب استخدام الموافقة مقابل القواعد القانونية الأخرى، حيث يركز النقاش بشكل عام على التحديات الحقيقية لتأمين الموافقة المستنيرة فعلاً والطوعية والقابلة للإلغاء في البيئات الإنسانية بسبب ديناميكيات القوة في المواقف الإنسانية (بما في ذلك المساعدات النقدية والقسائم) ونقص الاختيار وصعوبة شرح كيفية معالجة البيانات ومشاركتها من بين جوانب أخرى. أدى هذا النقاش جنبًا إلى جنب مع مزيد من الدراسة للأنظمة مثل النظام الأوروبي العام لحماية البيانات إلى قيام بعض المنظمات باستخدام إما المصالح المشروعة أو المهام / المصلحة العامة كأساس قانوني جنبًا إلى جنب مع نهج الموافقة المستنيرة الأخلاقية الإيجابية. انظر الصندوق 13 للحصول على شرح أكثر تعمقًا للأسس القانونية والإرشادات التي قد يكون الأساس القانوني هو الأنسب للمساعدات النقدية والقسائم. وتجدر الإشارة إلى أن هذا التوجيه لا يعمل كمشورة قانونية – بل يقصد به تقديم مجالات لاعتبارها من قبل مكتب حماية البيانات وفريقك القانوني عند اتخاذ قرار بشأن القواعد القانونية.

21 هذه القواعد القانونية مستمدة من اللائحة العامة لحماية البيانات في الاتحاد الأوروبي. ستحتاج إلى مراجعة التشريعات الوطنية لتحديد الأسس القانونية لبلد معين. تتمتع بعض المنظمات الدولية مثل الأمم المتحدة واللجنة الدولية للصليب الأحمر بامتيازات وحصانات وتتبع مبادئ وسياسات وعمليات وقواعد حماية البيانات الخاصة بها.

الصندوق 13: اختيار أساس قانوني لمعالجة لبيانات

لقد دارت نقاشات كثيرة حول قيود الموافقة المستنيرة كأساس قانوني لمعالجة البيانات في الحالات الإنسانية، حيث أن هناك رأي ناشئ وهو أن القواعد القانونية الأخرى قد تكون أكثر ملاءمة من الموافقة. نستكشف فيما يلي وجهة النظر الناشئة بالتفصيل.

بموجب النظام الأوروبي العام لحماية البيانات من غير المحتمل أن تكون بعض القواعد القانونية مناسبة للمساعدات النقدية والقسائم. على سبيل المثال من غير المرجح أن تكون المصالح الحيوية خيارًا قوياً حتى بالنسبة لحالات الاستخدام الإنساني،[22] وبالمثل لن تكون الأنشطة التنموية أو الإنسانية "مطلوبة بموجب القانون" بشكل عام مما يجعل "الالتزام القانوني" خياراً غير مرجح. نظراً لأن الوكالات عموماً لا تبرم عقوداً مع المجتمعات التي تعمل معها، فإن تنفيذ العقد (مع الأفراد) يعد خياراً غير محتمل.

يطرح هذا ثلاث قواعد قانونية للعمل الإنساني (بما في ذلك المساعدات النقدية والقسائم) تنقسم إلى مجموعتين رئيسيتين:
المجموعة 1 - الموافقة هي الأساس القانوني الوحيد الذي يضع الوكالة مقابل الفرد
المجموعة 2 - المهمة / المصلحة العامة والمصلحة المشروعة – تركز على الموازنة بين حقوق الأفراد واحتياجات المنظمات أو المجتمع ككل على النحو المعبر عنه من خلال قوانينه وعاداته

الموافقة

في حين أن استخدام الموافقة كأساس قانوني لا يلغي الحاجة إلى أن تكون المنظمات خاضعة للمساءلة أو آمنة أو تأخذ بعين الاعتبار المخاطر؛ فإن استخدامها يؤكد بشكل فعال أنه - في السياق الذي يتم فيه الحصول على الموافقة - يتمتع الأفراد بالصلاحيات الكافية لاتخاذ خيارات مستنيرة وطوعية. يحدد النظام الأوروبي العام لحماية البيانات أنه لكي يتمكن الأفراد من تقديم الموافقة يجب أن تكون المنظمات قادرة على تقديم خيار مستنير وقابل للإلغاء (قابل للعكس) في ظرف يمكن فيه حجبه أو رفضه دون عواقب سلبية.

هناك تحديات مختلفة لاستخدام الموافقة كأساس قانوني في السياقات الإنسانية أو التنموية؛ خاصة:

- نظراً لطبيعة الكثير من البرامج التي تركز على البيانات، فمن المحتمل أن تكون هناك عواقب إذا لم يوافق الشخص على تقديم البيانات - على سبيل المثال إذا لم يتم تقديم المساعدة دون التسجيل أو المشاركة
- من الصعب تقديم الاختيار الحقيقي أو الحر نظراً لاختلال توازن القوى الحالي لا سيما في السياق الإنساني
- سيكون من النادر تقديم "الحق في النسيان" أو سحب الموافقة - لا سيما عندما تكون هناك متطلبات أخرى مثل "اعرف عميلك" أو تحويل المساعدة أو التدقيق أو مكافحة الاحتيال أو المراقبة والتقييم والمساءلة والتعلم والتي قد تتطلب أن يتم الاحتفاظ بالبيانات الشخصية أو الحساسة وبالتالي منع "نسيان" الفرد

المصلحة القانونية / المهمة العامة / المصلحة العامة

حيثما لا يمكن عرض الخيار ولكن لا يزال النشاط مرغوباً به لتحقيق مهمة الوكالة أو لدعم منفعة اجتماعية معترف بها على أنها "مصلحة عامة" فقد تكون المصلحة القانونية أو المهمة العامة / المصلحة العامة بمثابة الأساس القانوني المناسب.

قد لا يبدو أن المصلحة القانونية أو المهمة العامة / المصلحة العامة ينتميان معاً لكن كلاهما يمثل "مصلحة" أو أمرًا ضروريًا كما هو موضح أدناه:

- قد يكون للمنظمة (المصلحة القانونية) مصلحة في دعم الضرورات الإنسانية أو الأهداف البرامجية المنصوص عليها في ميثاق المنظمة أو الوثائق التأسيسية أو المهمة أو الأهداف الخيرية - على سبيل المثال قد يكون للمؤسسة "مصلحة قانونية في خدمة الأهداف الخيرية من خلال تقديم أعمال منقذة للحياة للمجتمعات من خلال تقديم المساعدة العينية من خلال إعداد برامج المساعدات النقدية والقسائم التي تطلب اسم المستلم ووضعه من أجل تقييم هذه المساعدة وتقديمها"؛
- القانون والمجتمع (المهمة العامة / المصلحة العامة): قد ينشأ "أساس المصلحة العامة" من التمويل المؤسسي من المانحين الوطنيين مع تفويض صريح في القانون لتقديم المساعدة المنقذة للحياة

لا تتجاوز مبررات المصلحة القانونية أو المهمة العامة / المصلحة العام لجمع البيانات الالتزامات الأخرى في القانون أو الممارسات الجيدة لحماية البيانات. يبقى الالتزام بإبلاغ الأفراد لاستخدام "تحديد الغاية" ضئيلاً وآمنًا؛ وفي الواقع فإن النظام الأوروبي العام لحماية البيانات واضح في أنه إذا كانت هناك طريقة أخرى لتحقيق نفس النتيجة (أي إذا كنت لا تحتاج إلى بيانات) فلن يكون الأساس القانوني سارياً.

سيكون الاختيار النهائي للأساس القانوني في معظم الحالات عبارة عن مزيج من الظروف المحددة للمؤسسة والسياق القانوني المحلي (لا سيما إذا كان الموقف غير متعلق بالنظام الأوروبي العام لحماية البيانات وكان السياق أكثر ثنائية) وتفسير القانون. **لكننا نقترح أن عدم توازن القوة والاحتياجات الخارجية مثل "اعرف عميلك" والسياقات الصعبة والمتغيرة جميعها تجعل الموافقة غير مناسبة لمعظم الحالات إن لم يكن جميعها.**

22 يوضح السرد 46 أنه من المرجح أن تنطبق المصالح الحيوية فقط في نطاق ضيق من حالات "إنقاذ الحياة"، حيث لا يمكن أن تستند المعالجة بشكل واضح إلى أساس قانوني آخر. كما يحدد السرد 46 بوضوح "الأغراض الإنسانية" كمثال على المعالجة التي قد تخدم المصلحة العامة والمصالح الحيوية بما في ذلك مراقبة الأوبئة وانتشارها أو في حالات الطوارئ الإنسانية، حيث يشير هذا بوضوح إلى أنه بالنسبة لمعظم تدخلات الرعاية غير الحرجة، من غير المحتمل أن تكون الاهتمامات الحيوية اختيارًا جيدًا للعاملين في المجال الإنساني.

الصندوق 13: اختيار أساس قانوني لمعالجة لبيانات

قد يقدم نهج "المصلحة" (أي المهمة العامة / المصلحة العامة أو المصلحة القانونية) جنبًا إلى جنب مع نهج الموافقة الإيجابية والمستنيرة أخلاقياً، أفضل ما في كلا الجانبين؛ من خلال:

- الحفاظ على معايير عالية للاختيار للأفراد بناءً على صورة مناسبة وكاملة وحساسة للسياق لكيفية استخدام البيانات ولأي غرض
- وضع عبء أكبر على المنظمات لتكون وتبقى مسؤولة وتعكس سلوكياتها ، والمخاطر التي يعرضونها للمشاركين وكيف يمكن أن تتغير بمرور الوقت
- تعزيز الحاجة إلى الحكم والفهم السياقي - في التخطيط ووضع السياق وفي التصرف ورد الفعل

دمج الخصوصية في التصميم

بينما أشارت الوثيقة الإرشادية 1 إلى أهمية العمل ضمن مبادئ عالية المستوى للبيانات المسؤولة، فإن النظام الأوروبي العام لحماية البيانات – ومؤيدي الخصوصية - يوصون على وجه التحديد بدمج مبادئ الخصوصية حسب التصميم في مرحلة التصميم والتخطيط. تتمثل الفرضية الكامنة وراء الخصوصية في التصميم في أنه لا يمكن ضمان الخصوصية إلا من خلال الالتزام بالسياسة والأطر التنظيمية، كما يجب أيضاً دمجها في تصميم عمليات جمع البيانات بحيث تتناسب قوة إجراءات الخصوصية مع حساسية البيانات التي يتم جمعها ومعالجتها.[23] يجب أن تكون الخصوصية هي الوضع الافتراضي في كيفية تصميم عمليات البيانات وليس خيارًا يجب على الأشخاص اختياره. تعتبر النقاط الموجودة في الصندوق 14 بمثابة تذكير مفيد بكيفية التصميم مع دمج الخصوصية.

الصندوق 14: 7 مبادئ أساسية توجه عملية دمج الخصوصية في التصميم

1. **استباقية لا تفاعلية:** وقائية لا علاجية. توقع المخاطر وقم بمنع الأحداث والأضرار التي تنتهك الخصوصية قبل حدوثها وصمم استراتيجيات التخفيف من البداية
2. **الخصوصية كإعداد افتراضي:** لا يتعين على الفرد اتخاذ أي إجراء من أجل حماية خصوصيته. الخصوصية هي الوضع الافتراضي المدمج لجميع الإعدادات
3. **الخصوصية المتضمنة في التصميم:** تم تضمين الخصوصية في تصميم وهيكلة كل من الأنظمة والممارسات التجارية. الخصوصية هي عنصر أساسي للوظيفة الأساسية التي يتم تقديمها
4. **التوظيف الكامل:** قيمة موجبة وليس قيمة صفرية. لا يُجبر الأفراد على الاختيار بين الخصوصية واستخدام تطبيق أو أداة أو منصة أو خدمة. لا يعد التخلي عن الخصوصية شرطًا للحصول على المنتج
5. **الأمن الشامل:** حماية دورة الحياة الكاملة. يتم تمكين الخصوصية من خلال حماية سرية البيانات طوال دورة حياة البيانات. يتم جمع جميع البيانات واستخدامها والاحتفاظ بها وتخزينها بشكل آمن ثم إتلافها بشكل آمن في نهاية العملية في الوقت المناسب
6. **الرؤية والشفافية:** أبق الأمر مفتوحاً. يجب أن تعمل أي ممارسة أو تقنية عمل وفقًا للوعود والأهداف المعلنة مع مراعاة التحقق المستقل. يتم جعل أصحاب البيانات على دراية كاملة بالبيانات الشخصية التي يتم جمعها وماذا يتم بها ولأي غرض (أغراض) ومن قبل من.
7. **احترام خصوصية المستخدم:** اجعل العملية تتمحور حول المستخدم. يعطي المهندسون والمشغلون الأولوية لمصالح الفرد من خلال تقديم تدابير مثل الإعدادات الافتراضية القوية للخصوصية والإشعار المناسب وتمكين الخيارات سهلة الاستخدام. من المهم أيضاً الاستماع إلى المستخدمين والرد على ملاحظاتهم.

راجع هذه النبذة العامة لمزيد من المعلومات حول الخصوصية حسب التصميم

23 https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf

بذل العناية الواجبة في شركاء القطاع الخاص بما في ذلك مقدمي الخدمة المالية والأطراف الثالثة الأخرى

نظرًا لأن البيانات والأدوات الرقمية أصبحت جزءًا لا يتجزأ بشكل متزايد من العمل اليومي للمنظمات الإنسانية ولأن البيانات أصبحت أكثر تعقيدًا وتتطلب مهارات لا تمتلكها العديد من المنظمات حتى الآن؛ فإن الشراكات مع القطاع الخاص أصبحت بشكل متزايد جزءًا من كيفية إدارة المنظمات للبيانات. في بعض الأحيان تجلب هذه الشراكات التمويل أو الخبرة الفنية العينية معها، وفي أوقات أخرى فإنها تتيح مبادرات واسعة النطاق وأكثر استدامة مما يجعلها جذابة للقطاع الإنساني.

يتم أيضاً تقديم المساعدات النقدية والقسائم بشكل متزايد عبر مزودي الطرف الثالث. قد يكون لهذه الكيانات مصلحة في القيام بالأمر الجيد ومع ذلك فإن دافعها الأساسي هو الربح، كما قد يكون لديهم أيضاً التزامات بمشاركة البيانات بموجب قوانين مكافحة الإرهاب أو مكافحة غسل الأموال والتي قد تؤثر على كيفية تعاملهم مع البيانات. في بعض الحالات سيأخذ القطاع الخاص خصوصية البيانات وأمنها على محمل الجد من أجل الحفاظ على ثقة العملاء، وفي حالات أخرى، قد يكون لدى الجهات الفاعلة في القطاع الخاص مصلحة في تسييل البيانات أو إعادة استخدام بيانات العملاء لتطوير المنتجات والخدمات التجارية. إذا كنت قد أجريت تحليلاً للاقتصاد السياسي للبيانات (انظر الوثيقة الإرشادية 1)، فيجب أن يكون قد حدد بعض ديناميكيات القوة والدوافع المحتملة لشركاء القطاع الخاص في المساعدات النقدية والقسائم. في مرحلة "مشاركة البيانات" (الوثيقة الإرشادية 6) فإننا نناقش كيفية إعداد اتفاقيات لحماية بيانات متلقي المساعدات النقدية والقسائم والبيانات المؤسسية أثناء برامج المساعدات النقدية والقسائم.

هناك العديد من المنظمات الإنسانية لديها عمليات بذل العناية الواجبة القائمة، حيث تتضمن بعض جوانب مسؤولية البيانات الرئيسية التي يجب تضمينها في هذه العمليات ضمان أن شركاء القطاع الخاص:

- قادرون وراغبون في حماية البيانات بالطريقة التي يطلبها الفاعلون الإنسانيون
- لديهم سياسات وممارسات قوية ومسؤولة تحمي البيانات وتؤمّنها
- استجابت بطريقة مناسبة لانتهاكات البيانات السابقة أو حوادث البيانات
- لديهم خطوط أعمال ونماذج أعمال سابقة وحالية ومستقبلية تتوافق مع الأهداف الإنسانية الأساسية ومبادئ "عدم إلحاق الضرر"
- لا تشارك في الأنشطة التجارية التي تضر بالفئات السكانية المهمشة التي تهدف الوكالات الإنسانية إلى دعمها (مثل استخدام البيانات لتحديد اللاجئين والمهاجرين من أجل احتجازهم وترحيلهم وإنشاء تقنيات مراقبة تستخدمها الحكومات لاستهداف معين المجموعات السكانية للإجراءات الضارة أو بناء نماذج البيانات التي تُستخدم لاستبعاد الأشخاص المعرضين للخطر أو مجموعات معينة من المزايا والخدمات)
- تلتزم التزاماً راسخاً بالعمل مع برامج المساعدات النقدية والقسائم والمستفيدين بطرق ليست مفترسة أو استغلالية

بعض شركاء القطاع الخاص مثل العديد من مشغلي شبكات الهاتف المحمول لديهم نماذج أعمال تعتمد على إدارة البيانات الآمنة وبالتالي لديهم خبرة واسعة في مجالات خصوصية البيانات وأمنها، وفي بعض الحالات يمكنهم مساعدة المنظمات الإنسانية على التحسين في هذا المجال.

إذا كنت ستعمل مع القطاع الخاص بشأن البيانات أو المبادرات التقنية؛ فيمكنك استخدام **هذه المذكرة الإرشادية** لمساعدتك في تأطير شراكة تحمل مسؤولية البيانات في المركز.

يمكن أن تساعدك **قائمة التحقق القابلة للطباعة هذه من Electronic Frontier Foundation** على تقييم أمان بيانات الشريك وقدرة الخصوصية

يمكن أن تساعدك هذه **المجموعة المكونة من 7 أسئلة** في طرح الأسئلة الصحيحة على البائع حول الامتثال للنظام العام لحماية البيانات.

إنشاء عملية حوكمة البيانات للمساعدة في إدارة المسؤولية والمساءلة عن البيانات

بالاعتماد على هيكلية برنامج المساعدات النقدية والقسائم والشركاء المعنيين؛ من المهم توثيق من يتحمل المسؤولية عن إدارة البيانات بشكل عام ولكل عملية جمع بيانات في المراحل المختلفة من دورة برنامج المساعدات النقدية والقسائم، حيث يتضمن ذلك:

- الاحتفاظ بقائمة جرد البيانات وتتبع الشركاء الذين يحتفظون بالبيانات والتأكد من امتثالهم للأطر الزمنية للاحتفاظ بالبيانات وإتلافها والامتثال لاتفاقيات مشاركة البيانات واللغة الأخرى في العقود والاتفاقيات المتعلقة بحفظ البيانات والاحتفاظ بها وإتلافها
- تتبع من يمكنه الوصول إلى البيانات بما في ذلك إدارة التغييرات في مستويات الوصول للموظفين والشركاء
- ضمان تصنيف البيانات أو تعميمها في أسرع وقت ممكن بعد جمعها أو استخدامها (حسب الظروف)

- إدارة والاستجابة لأي طلبات من المشاركين في برنامج المساعدات النقدية والقسائم لتصحيح البيانات أو حذفها أو إزالتها من النظام.

تأكد من تحديد احتياجاتك المتعلقة بحفظ البيانات والاحتفاظ بها في المراحل الأولى من التخطيط الخاص بك للتأكد من أن لديك الميزانية اللازمة لحفظ البيانات والاحتفاظ بها وإتلافها بشكل آمن، حيث سيحدد دورك في المشروع ما إذا كانت هذه التكلفة تتحملها مؤسستك أو الشريك.

الإعداد لحوادث أو انتهاكات البيانات الحساسة المحتملة

تشمل حوادث البيانات الخطيرة انتهاكات البنية التحتية والكشف غير المصرح به أو تغيير البيانات واستخدام البيانات التي تم جمعها لأغراض إنسانية لغايات أخرى دون موافقة أو اتفاق مقابل، وهي تحدث عندما تتسبب الطريقة التي تُدار بها البيانات في إلحاق الضرر بالسكان المتضررين أو المنظمات أو الموظفين أو غيرهم من الأفراد أو المجموعات. يمكن أن تنطوي حوادث البيانات على سرقة أو مصادرة جهاز حاسوب محمول يحتوي على بيانات حساس، أو تغيير قائمة متلقي المساعدات النقدية والقسائم أو مشاركتها دون إذن أو تقديم مسح أو بيانات على مستوى الأسرة إلى السلطات. يمكن أن تحدث حوادث البيانات حتى بدون اختراق البنية التحتية التقنية، وعندما يؤدي جمع البيانات واستخدامها ومشاركتها إلى انتشار شائعات سلبية وحساسيات ثقافية وديناميكيات سياسية وعوامل أخرى لها آثار سلبية على السكان المتضررين أو المنظمات الإنسانية فيمكن اعتبار ذلك أيضاً بمثابة حادث بيانات بالغ الأهمية.[24]

بناءً على السياق العام وتقييم القدرات الخاص بك (الوثيقة الإرشادية 1) والتجارب السابقة وأنواع الجهات الفاعلة التي قد تكون مهتمة بالوصول إلى بياناتك؛ قم بإعداد قائمة بأنواع حوادث البيانات التي قد تحدث أثناء استجابة المساعدات النقدية والقسائم وقم بالتخطيط لكيفية تخفيفها في التخطيط والتصميم الخاص بك. ستحتاج إلى إثارة هذه المشكلة مع المنظمات الشريكة أو (إذا كنت تمثل منظمة منفذة) مع الوكالات التي تدير أنظمة البيانات، **وعند فحص الشركاء (مثل مقدمي الخدمات المالية وشركات تشغيل شبكات الهاتف المحمول وما إلى ذلك) الذين سيديرون أدوات البيانات الرقمية وأنظمة البيانات الأوسع نطاقًا؛ فمن المهم أن تكون مسئولياتهم (ومسؤولياتك!) عن حوادث البيانات الهامة مكتوبة كجزء من الاتفاقية التعاقدية الخاصة بك**، ويجب أن يشارك فريق أمن المعلومات الخاص بك لدعم هذا النوع من التدقيق ويمكن لفريقك القانوني توفير نماذج أو صياغة يجب تضمينها، ومن المحتمل أن تحتاج إلى إشراك مسؤول حماية البيانات أيضاً.

أخيراً؛ سترغب بتحديد كيفية تنظيمك للاستجابة لحادثة بيانات حرجة تم الإبلاغ عنها - وتوثيق ذلك في "بروتوكول حوادث البيانات الحرجة" الذي يحدد كيفية الإبلاغ عن حوادث البيانات والتحقيق فيها والإبلاغ عنها، كما سيحدد أيضاً العملية التي ستمضي بها لتحديد ما إذا كنت ستقدم تعويضاً أو دعماً لأي شخص يتضرر من خرق البيانات وكيفية ذلك. تتطلب معظم تشريعات خصوصية البيانات الإبلاغ عن خرق البيانات إلى سلطات حماية البيانات والمتأثرين به خلال إطار زمني محدد، في حين أنه كان من غير المألوف بالنسبة للجهات الفاعلة الإنسانية الكشف عن حوادث البيانات الخطيرة أو انتهاكات البيانات للسكان المأثرين حيث أن للأشخاص الحق في معرفة ما إذا كانت بياناتهم قد تعرضت للاختراق وأنواع الضرر الذي قد ينتج عن ذلك وأن يتم تعويضهم عن الأضرار التي قد يتعرضون لها. . ترتبط هذه المنطقة بالمساءلة تجاه السكان المتأثرين في مجال المساعدات النقدية والقسائم وبالتالي قد تكون الفرق العاملة على المساءلة تجاه السكان المتأثرين بمثابة حلفاء جيدين في هذا العمل. تعد فرق الحماية أيضاً بمثابة حلفاء ممتازين مع الأخذ في الاعتبار أن حوادث البيانات الحرجة تنطوي على ديناميكيات القوة والضرر، وتتحمل المنظمات مسؤولية منع حوادث البيانات وواجب العناية في الحالات التي تحدث فيها.

ستحتاج استراتيجيات التخفيف من حوادث البيانات الخاصة بك إلى تغطية أمن البيانات وأنظمة البيانات بالإضافة إلى تدريب وتحفيز الأشخاص لحماية البيانات، حيث سيتطلبون مدخلات من الموظفين ومسؤولي التعداد وغيرهم ممن يديرون البيانات "على أرض الواقع" والذين هم على دراية بالسياق اليومي للاستجابة.

تحدث مع فرق الحماية والأمن السيبراني وإدارة البيانات وحماية البيانات والشؤون القانونية والاتصالات / العلاقات العامة والامتثال لتحديد كيفية الاستجابة الجماعية لحوادث البيانات الهامة وما إذا كانت السياسات من هذا النوع موجودة بالفعل. قد تكون قادراً على البناء على خبرات وبروتوكولات حماية مؤسستك أو إدارة أزمات العلاقات العامة للتخطيط وإدارة حوادث البيانات الحساسة.

تأكد من تضمين حوادث البيانات الحساسة حول المخاطر - الفوائد - الأضرار أو تقييم تأثير خصوصية البيانات (انظر الخطوة التالية في الوثيقة الإرشادية هذه)، إلى جانب أمثلة حول كيفية تخفيف الأضرار المحتملة.

24 مركز تنسيق الشؤون الإنسانية للبيانات الإنسانية. ملاحظة رقم 2: إدارة حوادث البيانات. "سلسلة المذكرات الإرشادية: البيانات المسؤولة قيد التنفيذ" 2019

بعد تخطيط دورة حياة البيانات الكاملة (الوثائق الإرشادية 1 – 7) قم بإجراء تقييم لأثر خصوصية البيانات

تقييم تأثير خصوصية البيانات (يسمى أيضاً بتقييم تأثير الخصوصية أو PIA أو يُشار إليه أحيانًا باسم تقييم المخاطر – المنافع أو RBA) هو تحليل منهجي لمخاطر الخصوصية المحتملة التي يتعرض لها الأفراد بسبب جمع البيانات و استخدامها أثناء تنفيذ البرنامج.

يجب تنفيذ تقييم تأثير خصوصية البيانات خلال مرحلة التخطيط ولكنك ستحتاج إلى خطط قائمة من أجل دورة حياة البيانات الكاملة (المراحل 1 – 7) قبل حصولك على المعلومات اللازمة لإجرائه

يركز تقييم تأثير خصوصية البيانات بشكل واضح على الأضرار المحتملة للأشخاص الذين يتم جمع بياناتهم ومعالجتها - فهي ليست أداة لتقييم المخاطر والمسؤوليات التنظيمية. ومع ذلك إذا كان هناك خطر كبير لإلحاق ضرر بالأفراد والجماعات الذين يشاركون في برنامج ما، فإن المنظمة سوف تتراكم عليها المخاطر والمسؤولية. يسمح لك تقييم تأثير خصوصية البيانات بتحليل التهديدات والمخاطر المتعلقة بتأثير البيانات وتطوير استراتيجيات التخفيف، كما تساعد تقييمات تأثير خصوصية البيانات العاملين في المجال الإنساني على حماية خصوصية المشاركين وتقوية ثقة الجمهور في البرنامج. ينص النظام الأوروبي العام لحماية البيانات وبعض الأطر القانونية الأخرى على إجراء تقييم تأثير خصوصية البيانات أو تقييم تأثير الخصوصية في أي حالة يحتمل فيها وجود مخاطر عالية على السكان المستهدفين. يساعد تقييم تأثير خصوصية البيانات المنظمات على تحديد ما إذا كانت الفوائد المحتملة لجمع البيانات تفوق الأضرار المحتملة كما يوفر طريقة لتوثيق النتائج. يجب إجراء تقييم تأثير خصوصية البيانات بغض النظر عن طريقة تقديم المساعدات النقدية والقسائم.

إذا تم تدقيق مؤسستك من حيث ممارسات إدارة البيانات الخاصة بها فإن إجراء تقييم تأثير خصوصية البيانات يساعدك على توفير وثائق حول كيفية قيام مؤسستك بتحديد وتخفيف مخاطر جمع البيانات ومعالجتها. حيثما يمكن إظهار أن مؤسستك كانت شاملة في إدارة البيانات وتقليل المخاطر فمن المحتمل أن تكون الأحكام والغرامات أصغر. إذا كان يُعتبر بأن مؤسستك تتصرف بإهمال، فيمكن عندئذٍ التوصية بغرامات أعلى. إذا لم يتم إجراء تقييم تأثيرات خصوصية البيانات فمن المهم أيضاً توثيق أسباب عدم إمكانية ذلك.

يجب استخدام تقييم تأثيرات خصوصية البيانات كأداة تخطيط جنبًا إلى جنب مع عمليات تقييم المخاطر الأخرى لمؤسستك (أو دمجها فيها) من أجل تحديد مجالات الخطر لمؤسسة من حيث كيف يمكن أن تضر إدارة بياناتها بالسكان المتضررين وسمعتها الخاصة أو الوضع القانوني والمالي. ويجب أن تكون تقييمات تأثيرات خصوصية البيانات قدر الإمكان أنشطة تشاركية بحيث يتم تضمين آراء السكان المتأثرين في تحديد المخاطر وتأهيلها وفي اقتراح استراتيجيات التخفيف. يجب دمج أسئلة فحص تقييم تأثيرات خصوصية البيانات (مثل "هل هذه الفئة من السكان مهمشة؟") في عمليات أخرى مثل قوائم مراجعة التخطيط وأدلة تصميم البرنامج وأطر عمل الخروج وعمليات الموافقة على العطاءات للمساعدة في تعميم الخصوصية في المؤسسة الأوسع.

إذا وجدت المنظمة أثناء عملية تقييم تأثيرات خصوصية البيانات بأن الدعم والموارد المناسبين غير متاحين لإدارة البيانات بمسؤولية ولا يمكن جمع البيانات واستخدامها بشكل مسؤول بسبب السياق أو أن السكان المتضررين يتعرضون لمخاطر من استخدام البيانات بما لا يتناسب مع الفوائد؛ فيجب إيقاف الاستجابة وتنفيذ نهج برامجي مختلف أقل ثقلاً في البيانات.

ستقوم بعض المنظمات بتنفيذ تقييم تأثيرات خصوصية البيانات كجزء من هيكليات وأطر عمر الحوكمة الخاصة بها أيضاً. الأمر المهم هو أن يكون هناك تقييم مخاطر محدد يركز على البيانات ويركز على تأثير استخدام البيانات على السكان المتأثرين.[25]

بينما تقترح الوثيقة الإرشادية 1 تقييماً سريعاً لتحديد ما إذا كان يجب على المنظمة المشاركة بشكل عام في الاستجابة بناءً على السياق والقدرات (انظر الصندوق 9)، فإن تقييم تأثيرات خصوصية البيانات يتعمق في تقييم أنشطة جمع واستخدام البيانات المقترحة على النحو المحدد في خطة الاقتراح أو ممارسة جمع البيانات واستخدامها ضمن الاقتراح (على سبيل المثال عملية جمع البيانات لاستهداف المساعدات النقدية والقسائم أو استخدام طريقة تقديم المساعدات النقدية والقسائم المعينة أو عملية المسح أو المراقبة والتقييم والمساءلة والتعلم).

تتضمن الأمثلة على أطر عمل وعمليات تقييم تأثيرات حماية البيانات وتقييم تأثيرات الحماية وتقييم المنافع مقابل المخاطر:

- **دليل حماية البيانات** التابع للجنة الدولية للصليب الأحمر، الملحق 1، الصفحة 299
- **ورشة عمل إطار عمل تقييم مخاطر منافع** سونجارا

25 يمكن إجراء تقييم تأثيرات حماية البيانات في مراحل مختلفة من دورة برنامج المساعدات النقدية والقسائم، وقد يتم إجراء تقييم شامل للبيانات المتعلقة بالخصوصية في مرحلة تصميم البرنامج للمساعد في تحديد ما إذا كانت الجهات الفاعلة في المساعدات النقدية والقسائم قادرة على تقليل مخاطر الخصوصية إلى مستوى مقبول. يجب ألا تفوق المخاطر المحتملة على السكان المتضررين الفوائد المحتملة. الشيء نفسه ينطبق على المنظمات - يجب أن تحقق عمليات جمع البيانات فائدة أكبر من المخاطر، كما يجب أيضًا إجراء تقييمات حماية البيانات الشخصية لأنشطة محددة لجمع البيانات طوال دورة البرنامج. إذا تم استخدام نسق معياري لتقييم الأثر البيئي والاجتماعي، فيمكن تنفيذ تقييمات الأثر البيئي والاجتماعي بشكل دوري وبطريقة لامركزية في بداية أنشطة جمع البيانات الجديدة. يمكن دمجها واستخدامها بشكل دوري للتعلم والتحسينات بمرور الوقت. يجب أن تكون "وثيقة حية" تتم مراجعتها دوريًا، على سبيل المثال في حالة تغيير الشركاء أو السياق أو استخدام البيانات.

- وثيقة **أداة تقييم مخاطر المنافع** التابعة للوكالة الأمريكية للتنمية الدولية، الصفحات 11-13 من اعتبارات استخدام البيانات بمسؤولية
- **مفوض الخصوصية لدى PIA بنيوزيلندا**
- **حماية خصوصية المستفيدين** من شراكة التعلم النقدي، الصفحات 19-20
- إطار عمل مايكروسوفت **لتقييم الضرر لمنشئي التكنولوجيا**

تستخدم بعض المنظمات تقييم المخاطر والمنافع والذي يمكن أن يكون أكثر فائدة للسياق الإنساني وطالما أنه يغطي جوانب خصوصية البيانات، فإنه غالبًا ما يحل محل تقييم تأثيرات خصوصية البيانات. يفحص تقييم المخاطر والمنافع للبيانات السؤال الحاسم حول من يخاطر ومن يستفيد من جمع البيانات في محاولة للتأكد من أن الفئات الأكثر تهميشاً لا تتحمل المخاطر بينما تجني المؤسسات الفوائد. تغطي **مذكرة مكتب تنسيق الشؤون الإنسانية** حول تقييمات تأثير البيانات الأنواع المختلفة من التقييمات وكيفية تحديد الأنسب في أي إعدادات.

3 الوثيقة الإرشادية

جمع أو الوصول إلى البيانات

يمكن استخدام البيانات لأغراض جيدة مثل تحسين استهداف البرامج وتقليل الازدواجية والاحتيال، كما يمكن استخدامها أيضاً للتأثير على السلوكيات بطرق غير شفافة: للابتزاز واستهداف الأفراد والجماعات على حد سواء لإلحاق الأذى الفعلي ونشر المعلومات المضللة، ويمكن أن تؤدي البيانات أيضاً عن غير قصد إلى ضرر على الرغم من النوايا الحسنة. لجميع هذه الأسباب ولأن الناس لديهم حق أساسي في الخصوصية؛ فمن الأهمية بمكان جمع البيانات والوصول إليها بشكل مسؤول.

يحدث جمع البيانات الشخصية وغيرها من أشكال البيانات الحساسة في كل مرحلة من مراحل برنامج المساعدات النقدية والقسائم بما في ذلك:

- التخطيط وتقييم الاحتياجات
- الاستهداف
- المشاركة والتسجيل
- التقديم
- التغذية الراجعة
- المراقبة والتقييم

تغطي الوثيقة الإرشادية 3 الجوانب التي ستساعدك على جمع بيانات عالية الجودة ضرورية ومتناسبة مع الغرض الذي تم جمعها من أجله. في الحالات التي تقوم فيها بالوصول إلى البيانات التي تم جمعها مسبقًا أو بواسطة مؤسسات أخرى، يجب أن يظل هذا الدليل ساريًا.

الصندوق 15: مفاهيم البيانات: البيانات الشخصية والبيانات الشخصية الحساسية والبيانات غير الشخصية الحساسية والبيانات الوصفية

ما هي البيانات الشخصية؟

- هي البيانات التي تتعلق بفرد محدد أو يمكن التعرف عليه، بما في ذلك البيانات التي تحدد هوية الفرد بشكل مباشر (اسم أو رقم أو عنوان IP أو معرف "ملف تعريف الارتباط") أو البيانات التي يمكن أن تحدد هوية الفرد (على سبيل المثال لأن مجموعة البيانات صغيرة أو لأن البيانات تتضمن معلومات أو مجموعة من المعلومات تجعل من السهل التعرف على فرد ضمن مجموعة بيانات أكبر)
- البيانات التي تحدد الفرد عند تقاطع مجموعة بيانات مع مجموعة بيانات أخرى

ما هي البيانات الحساسة؟

- تتضمن البيانات الحساسة بيانات شخصية حساسة والتي إذا تم الكشف عنها أو الوصول إليها دون تصريح مناسب يمكن أن تؤدي إلى التمييز أو القمع ضد الفرد أو مصدر المعلومات أو الأشخاص أو المجموعات الأخرى التي يمكن التعرف عليها.

الصندوق 15: مفاهيم البيانات: البيانات الشخصية والبيانات الشخصية الحساسية والبيانات غير الشخصية الحساسية والبيانات الوصفية

- تتضمن البيانات الشخصية الحساسة عادةً العرق والأصل الإثني والانتماء السياسي والدين ، والعضوية النقابية والمعلومات الوراثية والبيانات الحيوية والصحة والحياة الجنسية والتوجه الجنسي كما تتضمن أيضاً بيانات شخصية حول الأفراد المعرضين للخطر بشدة مثل الأطفال أو النازحين
- يمكن أن تكون المعلومات الشخصية الأخرى حساسة اعتماداً على السياق والثقافة، وفي السياقات الإنسانية تكون الكثير من البيانات شديدة الحساسية. نظرًا لأن البيانات تحتوي على مستويات مختلفة من الحساسية اعتمادًا على السياق، فإننا لا نحدد قائمة نهائية بنقاط البيانات الحساسة في مجموعة الأدوات هذه
- من الجيد التفكير في من يقرر ما هو حساس أم لا. قد تحدد المجتمعات المتأثرة أن حقل بيانات معينًا حساسًا حتى عندما لا تصنفه أنظمة خصوصية البيانات أو المنظمات المنفذة على أنه حساس

ما هي البيانات غير الشخصية الحساسة؟

- بيانات حول السياق الذي تحدث فيه الأزمة (على سبيل المثال معلومات حول المجتمعات التي تتلقى المساعدات النقدية والقسائم)
- بيانات حول استجابة المنظمات والأشخاص الذين يسعون إلى المساعدة (على سبيل المثال مواقع توزيع النقد أو خطط تمارين جمع البيانات)[26]

ما هي البيانات الوصفية؟

- البيانات الوصفية هي "بيانات حول البيانات"
- يتم إنتاج البيانات الوصفية من خلال الترتيبات العملية للمساعدات النقدية والقسائم وتنطبق الالتزامات القانونية والتنظيمية المختلفة على جمع البيانات الوصفية ومشاركتها والاحتفاظ بها
- في حالة الأموال عبر الهاتف المحمول على سبيل المثال؛ تتضمن البيانات الوصفية أرقام هواتف المرسل والمستلم وتاريخ ووقت العملية المالية ومعرّف العملية وموقع وحجم العملية والمتجر الذي تم إجراؤه فيه وأي وكلاء مشاركين في أي من الطرفين
- يمكن استخدام هذه البيانات لاستنتاج معلومات واستخبارات أخرى، والتي يمكن استخدامها لتحديد هوية المستخدمين واستهدافهم ومراقبتهم. يمكن استخدامها لاستنتاج معلومات حول سلوكيات السكان المتأثرين وحركاتهم وانتماءاتهم وخصائص أخرى. إن القدرة على استخلاص استنتاجات بشأن المستفيدين ممكنة بعد فترة طويلة من انتهاء البرنامج[28,27]

حدد كيفية حماية البيانات إذا كنت تقوم بجمعها عن بعد أو عبر الهاتف المحمول

بينما تتم ممارسة جمع البيانات عن بعد في بعض البلدان بسبب النزاع أو بيئات العمل الصعبة؛ أصبح هذا النوع من الجمع أكثر انتشارًا خلال جائحة كوفيد-19. لقد بدأت العديد من المنظمات في إجراء استهداف المساعدات النقدية والقسائم عبر المكالمات الهاتفية أو الاعتماد على أفراد المجتمع لتحديد وإدارة اختيار متلقيي المساعدات النقدية والقسائم. تنشأ مخاوف تتعلق بالسرية مع هذا النوع من جمع البيانات والتي يمكن أن تؤدي إلى المحسوبية أو التلاعب بالقوائم أو وضع أفراد المجتمع في موقف يضطرون فيه إلى إدارة طلبات النقد. إذا كان الجهد يتم عن بعد بالكامل فلن يكون هناك طرف ثالث خارجي متاح (مثل مؤسسة المساعدات النقدية والقسائم) للإبلاغ أو تقديم الدعم في هذه المواقف.[29] من ناحية أخرى، فقد تم سحب أو تقليل أنظمة اعرف عميلك في بعض الحالات وعندما يتم تنفيذها فقد وجدت المنظمات صعوبة في الامتثال لها عند تسجيل المستلمين عبر الهاتف لأنهم لم يتمكنوا من التحقق من الهوية بشكل مباشر. بينما لا يزال يتم جمع بعض هذه البيانات دون استخدام الآليات الرقمية عن بعد، إلا أن الجمع عن بعد هو مشروع سريع التطور مع العديد من الجهود الجديدة التي تنطوي على طرق جمع البيانات الرقمية. تشمل الأمثلة على الممارسات الجديدة المبتكرة التي تظهر استخدام التعريف الصوتي أو "صور السيلفي" لإثبات الهوية، حيث أشار فريق عمل الإجراءات المالية مؤخرًا إلى أن التحقق من الهوية عن بُعد يمكن أن يكون فعالًا بنفس القدر حيث يمكن تحقيق مستويات عالية من ضمان الهوية وهو ليس خيارًا يتعين على الأشخاص الاشتراك فيه. تعتبر النقاط الموجودة في الصندوق 14 بمثابة تذكير مفيد بكيفية التصميم مع تضمين الخصوصية.[30]

26 مكتب تنسيق الشؤون الإنسانية 2019 إرشادات مسؤولية البيانات: مسودة عمل
27 دليل حماية البيانات الصادر عن اللجنة الدولية للصليب الأحمر
28 اللجنة الدولية للصليب الأحمر ومنظمة الخصوصية الدولية 2018 مشكلة البيانات الوصفية الإنسانية: عدم التسبب بأي ضرر في العصر الرقمي
29 الوثيقة الإرشادية من منظمة إنقاذ الطفل "التعديلات في كيفية تحديد المستفيدين من المساعدات النقدية والقسائم وتسجيلهم والتحقق منها في وقت كوفيد-19 (غير منشورة)
30 مجموعة العمل المالي "الهوية الرقمية"

راجع **المساعدات النقدية والقسائم من شراكة التعلم النقدي في سياقات كوفيد-19** للحصول على نبذة عامة حول كيفية تكيف الوكالات المختلفة مع جمع البيانات عن بُعد والأنشطة البعيدة الأخرى.

راجع **هذه المناقشة** حول الإيجابيات والسلبيات والممارسات الجيدة للمراقبة عن بُعد.

راجع **قائمة التحقق** هذه للحصول على إرشادات حول كيفية جمع بيانات المحمول بأمان. يمكن تكييفها لجمع بيانات المحمول من أجل المساعدات النقدية والقسائم.

تقدم **مجموعة أدوات برنامج الأغذية العالمي لتحليل نقاط الضعف ورسم الخرائط** إرشادات حول إجراء استطلاعات الرأي المتنقلة بشكل مسؤول

استخدام طرق ومنهجيات وأدوات جمع البيانات الدامجة

عند تصميم جمع البيانات خاصةً في حالة استخدام الأدوات الرقمية؛ يعد التصميم الهادف للمج أمراً بالغ الأهمية لتجنب استبعاد الفئات السكانية الأكثر تهميشاً. إن حصول النساء على الهواتف المحمولة أقل مقارنة بالرجال وهذا صحيح بشكل خاص في السياقات الإنسانية. على سبيل المثال؛ أظهر تقرير الفجوة بين الجنسين في الهاتف المحمول لعام 2020 الصادر عن GSMA أن احتمالية امتلاك النساء للهواتف المحمولة أقل بنسبة 8% من الرجال وتزداد هذه الفجوة لتصل إلى 20% عندما يتعلق الأمر بالإنترنت عبر الهاتف المحمول ويمكن أن تكون تلك الفجوات أكبر في السياقات الإنسانية.[32] من المرجح أيضاً أن يتم استبعاد الأشخاص الأشد فقرًا من الحصول على الهاتف المحمول، وبالمثل من المهم للمنظمات أن تفكر فيما إذا كانت تشمل الأشخاص ذوي الإعاقة والمجموعات الأخرى التي تتعرض للتمييز. ستحتاج إلى بناء هذه الحالات المسماة "الحافة" في تصميم عملية جمع البيانات من البداية - والميزانية المخصصة لها، وهذا يعني اتخاذ خطوات للتصميم لأنواع مختلفة من الوصول والبحث بنشاط عن حالات "الحافة" للتأكد من أنك تختبر طرق وأساليب جمع البيانات مع تلك المجموعات التي من المرجح أن يتم استبعادها.

تحتوي **بوابة المساءلة والشمول هذه التابعة للجنة الدائمة المشتركة بين الوكالات** على موارد وأدلة لضمان الإدماج في العمليات الإنسانية.

راجع **مجموعة الأدوات** هذه بشأن ضمان شمول الأشخاص ذوي الإعاقة رقميًا.

تقدم **مجموعة أدوات النوع الاجتماعي وتكنولوجيا المعلومات والاتصالات** من الوكالة الأمريكية للتنمية الدولية عددًا من الوحدات والاعتبارات لفهم وصول المرأة إلى تكنولوجيا المعلومات والاتصالات.

ستحتاج إلى تقديم أكثر من خيار أو مسار واحد لجمع البيانات للتأكد من أن الأشخاص الأكثر تهميشاً (على سبيل المثال أولئك الذين لا يمكن الوصول إليهم بسهولة والنساء وأولئك الذين لا يتحدثون لغات أكثر شيوعاً) وذوي الإعاقة ليسوا مستبعدين.

اعتبار تأثير اعرف عميلك وتسجيل شريحة الهاتف المحمول وتدابير مكافحة الإرهاب

عندما تتعاون المنظمات الإنسانية مع مشغلي شبكات الهاتف المحمول وغيرهم من مقدمي الخدمات المالية، يتعين عليهم الامتثال لقواعد اعرف عميلك ومكافحة غسل الأموال وإجراءات مكافحة الإرهاب واللوائح والتشريعات الأخرى المصممة لمنع غسل الأموال والفساد؛ وهذا يعني أنه يجب على مؤسستك أو متلقيي المساعدات النقدية والقسائم مشاركة البيانات الشخصية والحساسة مع جهات خارجية بما في ذلك الجهات التنظيمية من أجل التحقق من هوية متلقي المساعدات النقدية والقسائم. تتطلب بعض الجهات المانحة فحصاً إضافيًا كجزء من تدابير مكافحة الإرهاب. بالإضافة إلى ذلك، هناك أكثر من 155 حكومة حول العالم لديها سياسات إلزامية لتسجيل شريحة الهاتف والتي تتطلب من الأشخاص تقديم إثبات الهوية قبل أن يتمكنوا من الحصول على شريحة.[33]

قد يقدم فريق عمل الإجراءات المالية، وهي الجهة الرقابية العالمية لغسيل الأموال وتمويل الإرهاب، توصيات إضافية وفي هذه الحالة يتم تحويل هذه التوصيات إلى القانون الوطني، ويجب فحص المستفيدين الجدد من المساعدات النقدية والقسائم مقابل هذه القوائم. يجب مراجعة معلومات "اعرف عميلك" مقابل القوائم التي وضعتها السلطات المحلية بما في ذلك الأفراد والكيانات التي يُحتمل أن تكون متورطة في نزاع أو حالة عنف. قد يتم استبعاد المستفيدين من المساعدات النقدية والقسائم من المساعدة إذا تم العثور على تطابق حتى لو كان التطابق حالة خطأ في الهوية. في حالات النزاع؛ قد تكون العائلات التي تحتاج إلى المساعدات النقدية والقسائم من المجتمعات الموجودة في هذه الأنواع من قوائم المراقبة، حيث يتم تصنيفها غالبًا حسب المنطقة الجغرافية.

يمكن مراقبة هذه العملية من قبل السلطات العامة وأن تشمل التزامات الإبلاغ. غالباً ما يتم تفعيل تدابير مكافحة الإرهاب وغسيل الأموال بمساعدة برامج طرف ثالث، ومع ذلك فإنه من غير الواضح أحيانًا ما يحدث للبيانات التي يتم إدخالها في قواعد البيانات هذه. يمكن استخدام البيانات التي تم جمعها لأغراض أخرى من قبل الحكومات أو مقدمي الخدمات المالية أو مشغلي شبكات الهاتف المحمول، مثل الإعلان عن خدمات مالية إضافية (أو خدمات أخرى في حالة بيع البيانات أو مشاركتها فيما بعد) أو تحديدات الجدارة الائتمانية.

31 النظام الدولي لاتصالات المحمول "فجوة النوع الاجتماعي في المحمول" 2020
32 النظام الدولي لاتصالات المحمول سد فجوة النوع الاجتماعي في المحمول 2020
33 النظام الدولي لاتصالات المحمول برنامج الهوية الرقمية GSMA: رؤى وإنجازات (2016-2020)

من الأهمية بمكان عند التفاوض على نطاق العمل وعملية التوريد مع مقدم الخدمات المالية أن يتم تقييم هذه العناصر المهمة وأن يكون لدى المنظمات عمليات واضحة مطبقة لمراجعة أي نطاق من وثائق العمل. يجب تنسيق هذه العملية بين الفرق التي تدير عمليات المساعدات النقدية والقسائم مباشرة وفرق التكنولوجيا التي يمكنها تقييم جوانب مثل الأمان وتخزين البيانات وعناصر الخادم ومسؤولي البيانات والخصوصية والمشتريات، حيث يمكن أن يساعد هذا المنظمات على تجنب الفجوات والثغرات أو المفاجآت، مثل بنود مشاركة البيانات التي لا تحمي بيانات المساعدات النقدية والقسائم بشكل كامل.

لا تتطلب جميع الجهات المانحة أو حكومات الدول هذا النوع من الفحص، ولكن في الحالات التي يكون فيها ذلك مطلوباً؛ يجب أن تفسر ذلك للأشخاص المتأثرين كجزء من عملية جمع البيانات ويجب أن يتم منحهم خياراً فيما إذا كانوا يريدون تقديم بياناتهم أو للتسجيل باستخدام نوع مختلف من العمليات أو لتلقي المساعدة بشكل آخر مثل العينية أو النقد المباشر أو القسائم لمرة واحدة أو البطاقات الذكية مجهولة المصدر. ومع ذلك، ليست كل الوكالات قادرة على اتخاذ هذا الاختيار لأنه يعتمد على هيكليتها وحجمها واعتمادها على الوكالات الأخرى للأنظمة والتمويل.

من الممكن التفاوض مع المانحين فيما يتعلق بالآثار التشغيلية لمتطلباتهم للفحص، حيث يدرك المانحون بشكل متزايد الحاجة إلى إدارة البيانات بمسؤولية وتخفيف المخاطر المتعلقة بالبيانات. غالباً ما يدركون المقايضات المشمولة مثل أن الفحص يقوض المبادئ الإنسانية للنزاهة؛ ما يعني أنه سيكون لديك مجال للتفاوض.

يمكن العثور **هنا** على قائمة بالدول التي تتطلب تسجيل شريحة الهاتف منذ 2020.

تمت مناقشة سياسة "اعرف عميلك" وبعض الأمثلة على اللوائح المعدلة في هذه **الوثيقة الإرشادية** من عام 2016.

العناية الإضافية لاعتبار تكاليف ومنافع جمع البيانات الحيوية أو تقديم أنظمة رقمية

يتم الاستشهاد بعدد من الفوائد عند استخدام البيانات الحيوية لإدارة وتتبع تسجيل وتقديم المساعدة الإنسانية بما في ذلك المساعدات النقدية والقسائم، كما يتم استخدام البيانات الحيوية مثل بصمات الأصابع ومسح قزحية العين والتعرف على الوجه والقياسات الحيوية للصوت كجزء من إعداد برامج المساعدات النقدية والقسائم في أجزاء مختلفة من العالم. إنها تقدم شكلاً واحدًا من أشكال التعريف الفريدة للفرد حتى لو لم تكن هناك وسيلة أخرى لإثبات هويتهم بسبب فقدان وثائق الهوية الأخرى الخاصة بهم أو عدم توفرها بطريقة أخرى (في كثير من الأحيان حالة النازحين). بينما تم الترويج للقياسات الحيوية كوسيلة للحد من الاحتيال الفردي؛ لاحظ النقاد أنها لا تعالج الفساد وإساءة الاستخدام الأوسع على المستوى النظامي، حيثما يُشتبه في حدوث معظم حالات الاحتيال. بالإضافة إلى ذلك فقد تم الاستفسار عن القياسات الحيوية لتقديم الكفاءات للوكالات دون تقديم فوائد إضافية للسكان المأثرين ولعدد من الأسباب الأخرى مثل عدم الدقة وخطر تغير الوظيفة وإمكانية مشاركة البيانات الحيوية مع الحكومات. تستكشف بعض المؤسسات استخدام تقنيات الحفاظ على الخصوصية وأنظمة التشفير وأنظمة السجلات الموزعة مثل blockchain كطريقة للاحتفاظ ببيانات القياسات الحيوية بشكل أكثر أمانًا ولكن هناك حاجة إلى مزيد من العمل في هذا المجال.

في حالة استخدام بيانات القياسات الحيوية، يجب أن تكون متناسبة مع الغرض الذي يتم جمعها من أجله ويجب أن تكون المؤسسات قادرة على إثبات أن الفائدة من استخدام القياسات الحيوية تفوق مخاطر استخدامها. نظراً للطبيعة الحساسة للغاية للقياسات الحيوية؛ ستحتاج دائماً إلى إجراء تقييم تأثيرات خصوصية البيانات أو تقييم تأثيرات الخصوصية أو تقييم المنافع مقابل المخاطر قبل تأكيد استخدام القياسات الحيوية. إذا كنت بصفتك وكالة منفذة مطالباً باستخدام القياسات الحيوية لأن النظام الذي تقوم بتزويد البيانات به يتطلب ذلك؛ فستحتاج إلى مراجعة قدرتك بعناية على جمع القياسات الحيوية وإدارتها بشكل آمن، ويجب على الوكالات التي تطلب من شركائها استخدام القياسات الحيوية التأكد من أن هؤلاء الشركاء لديهم القدرة على حماية البيانات الحيوية. نظراً لوجود مستوى من عدم الارتياح للقياسات الحيوية بين بعض المجتمعات المتأثرة، فمن الأهمية بمكان أن يتم منح الأفراد خيارًا مجانيًا وذا مغزى حول ما إذا كانوا سيقدمون القياسات الحيوية مقابل التسجيل في المساعدات النقدية والقسائم أو تلقيها وأنك توفر أيضاً بديلاً لا يشكل عبئاً على الفرد. يتم استكشاف أشكال التعريف الأخرى التي تخدم غرض الهوية الفريدة ولكنها لا تتضمن القياسات الحيوية من قبل منظمات مثل ميرسي كوربس. إذا كنت تستكشف استخدام القياسات الحيوية؛ فتأكد من فهمك الكامل لكيفية عمل حل معين من البداية إلى النهاية، وإذا كان الحل صعب الفهم، فقد يكون هذا سبباً كافياً للعودة إلى أشكال الهوية غير الحيوية. لقد أجرت اللجنة الدولية للصليب الأحمر استكشافاً متعمقًا للزمان والمكان المناسبين لاستخدام القياسات الحيوية وحددت بعض الحالات التي تكون فيها مناسبة وبعضها غير مناسب.

34 أوكسفام وThe Engine Room(2018) القياسات الحيوية في القطاع الإنساني

35 انظر الرسالة المفتوحة لـ Access Now حول "لماذا الهوية" لمزيد من المعلومات حول تحديات القياسات الحيوية في العمل الإنساني ومواقف أخرى

يقدم **Internal Primer** Mercy Corps إرشادات مفصلة بشأن القياسات الحيوية.

راجع الفصل الثامن حول القياسات الحيوية في **دليل حماية البيانات الصادر عن اللجنة الدولية للصليب الأحمر** للحصول على مناقشة شاملة للقياسات الحيوية وكيفية التعامل مع هذا النوع من البيانات الحساسة وبموجب أي أساس قانوني يمكن جمعها في ظروف مختلفة.

انظر **هذه الوثيقة** لمناقشة شاملة لاستخدام القياسات الحيوية وأنظمة تحديد الهوية والتسجيل في الأزمات الممتدة والمتكررة.

اقرأ هذه **"الرسالة المفتوحة الموجهة إلى قادة بنوك التنمية الدولية والأمم المتحدة ومنظمات المعونة الدولية ووكالات التمويل والحكومات الوطنية"** للحصول على مراجعة أكثر تعمقًا لبعض الأسئلة الأساسية والقضايا المتعلقة بأنظمة الهوية البيومترية

التواصل بشفافية مع السكان المتأثرين بشأن جمع ومعالجة البيانات

يعد التواصل الشفاف والواضح مع السكان المتأثرين بشأن جمع البيانات ومعالجتها بمثابة جزء مهم من أي عملية بيانات ويجب أن يكون جزءاً لا يتجزأ من كيفية تصميمك وتخصيص ميزانيتك لإدارة البيانات المسؤولة. كما هو مذكور في الوثيقة الإرشادية 2 في القسم الخاص بالقواعد القانونية (انظر الصندوقين 12 و 13 في الصفحتين 20 و 21)، فإن استخدام الموافقة كأساس قانوني لجمع البيانات ومعالجتها قيد النقاش. ومع ذلك، بغض النظر عن الأساس القانوني الذي تستخدمه لجمع البيانات ومعالجتها؛ ستحتاج لأن تكون قادراً على التوضيح بشفافية للمجتمعات المتأثرة (بطرق مناسبة ثقافياً) من المكلف بجمع البيانات وكيفية الاتصال بهم ولماذا يتم جمعها ومعالجتها ومن يجب الاتصال به في حالة وجود أي أسئلة حول معالجة البيانات ومع من ستتم مشاركة البيانات، خاصةً إذا كانت ستتم مشاركتها مع السلطات أو الهيئات الحكومية مثل إنفاذ القانون أو الكيانات في إقليم أو ولاية قضائية أخرى.

الصندوق 16: ما الذي يجب على السكان المتأثرين معرفته قبل تزويد بياناتهم؟

تنص سياسة اللجنة الدولية للصليب الأحمر على توفير المعلومات التالية للأفراد المتضررين عندما تكون الموافقة هي الأساس القانوني:

- هوية وتفاصيل الاتصال الخاصة بالمؤسسة التي فُوضت وتراقب جمع البيانات ومعالجتها ("مراقب البيانات")
- الغرض المحدد لمعالجة البيانات الشخصية
- شرح المخاطر والفوائد المحتملة لمعالجة البيانات
- أن المراقب يمكن أن يعالج البيانات الشخصية لأغراض أخرى مماثلة (حدد ما قد تكون هذه الأغراض)
- أنه يمكن سحب الموافقة في أي وقت
- الظروف التي قد لا يكون من الممكن فيها معالجة البيانات الشخصية بسرية
- حقوق الاعتراض على معالجة بياناتهم وحقوق الوصول إلى البيانات الشخصية وتصحيحها وحذفها
- كيفية ممارسة الحقوق المتعلقة بالبيانات والقيود المحتملة على ممارسة هذه الحقوق
- البلدان الثالثة أو المنظمات الدولية التي قد يتم نقل بياناتها إليها من أجل تحقيق الغرض من الجمع الأولي والمعالجة الإضافية
- كم من الوقت سيتم الاحتفاظ فيه بالبيانات الشخصية (أو المعايير التي سيتم استخدامها لتحديد المدة التي سيتم الاحتفاظ بها) وأي خطوات يتم اتخاذها لضمان دقة السجلات وتحديثها؛
- مع أي من المنظمات الأخرى مثل السلطات في بلد جمع البيانات، يمكن مشاركة بياناتها
- إشارة إلى التدابير الأمنية التي تنفذها وحدة مراقبة البيانات فيما يتعلق بمعالجة البيانات[36]

ستحتاج إلى تبسيط أي اتصال بشأن كيفية معالجة البيانات وتخزينها بلغة واضحة وسهلة الوصول وذات مغزى للأفراد والمجتمعات المتضررة. قد تساعد الرسومات ومقاطع الفيديو وعمليات الموافقة الصوتية ذلك، ويجب أن تدرك أن الموافقة الفردية والخصوصية هما مفهومان يترجمان بشكل مختلف وفقًا للثقافة

36 دليل حماية البيانات الصادر عن اللجنة الدولية للصليب الأحمر (2020).

انتقد بعض الموظفين الذين يعملون في المساعدات النقدية والقسائم الأساليب الأوروبية والقانونية للموافقة والخصوصية لكونها شمالية، ويُنظر إليها على أنها تفضيلية، وغالباً ما تكون غير مفيدة أو لا تحظى بالتقدير؛ نتيجة لذلك فإن أهم شيء عند السعي لتحقيق الشفافية حول جمع البيانات ومعالجتها هو التأكد من أن السكان المتأثرين يفهمون العملية تماماً بدلاً من مجرد إجراء تمرين على قائمة التحقق.

تأكد من تضمين معلومات حول جمع البيانات وحقوق البيانات وآليات الشكاوى في ملاحظاتك الإجمالية وعمليات المساءلة لأي برنامج من برامج المساعدات النقدية والقسائم، حيث يتضمن ذلك معلومات حول البيانات الوصفية (انظر التعريف في الصفحة 26) التي سيتم جمعها من خلال إعداد برامج المساعدات النقدية والقسائم الرقمية أو جمع البيانات.

يمكن أن تساعدك **مجموعة الأدوات هذه** في تصميم خطة اتصال وتواصل مسؤولة للبيانات من أجل استجابتك.

إذا كنت تقدم آلية للشكاوى - ويجب أن تكون كذلك! - تأكد من أنك قد خططت للموظفين وقدرة الأنظمة والميزانية لتنفيذها. على سبيل المثال إذا أراد شخص ما إزالة بياناته من نظامك فهل يمكنك العثور عليها في نظامك والتحقق من هويته والامتثال لطلبه؟

لمزيد من المعلومات حول الموافقة؛ راجع **وثيقة الموافقة المستنيرة** الخاصة بمنظمة وورلد فيجين.

راجع **دليل حماية البيانات** الصادر عن اللجنة الدولية للصليب الأحمر للحصول على مزيد من الأفكار حول كيفية إدارة الموافقة المستنيرة وغيرها من القواعد القانونية جنباً إلى جنب مع النماذج واللغة للتكيف مع وضعك. يقدم الفصل 9 من الدليل توجيهًا تفصيليًا حول المساعدات النقدية والقسائم وحماية البيانات أيضاً.

تعرف على المزيد حول **آليات الشكاوى المجتمعية المشتركة بين الوكالات**.

4 الوثيقة الإرشادية

نقل وتخزين البيانات

يحدث نقل البيانات عندما يتم تمرير البيانات بين مكان وآخر، على سبيل المثال عندما يقوم موظفو مؤسستك بتمرير البيانات أو الملفات لبعضهم البعض أو إلى مؤسسة أخرى أو إلى حكومة أو كيان آخر. في بعض الأحيان يكون نقل البيانات عملية نشطة؛ مثلاً عندما يضغط مسؤول التعداد على "إرسال" بحيث تنتقل بيانات المسح عبر شبكة الهاتف المحمول من الهاتف المحمول إلى خادم المؤسسة أو إلى النظام السحابي. في أحيان أخرى يحدث ذلك خلف الكواليس لأن هناك جهازًا محمولًا أو تطبيقًا أو موقعًا إلكترونيًا أو برنامجًا ينقل البيانات تلقائيًا أثناء استخدام شخص ما لها، على سبيل المثال عندما يتم نقل بيانات الموقع إلى مشغل شبكة الهاتف المحمول لأن الهاتف المحمول يتصل ببرج هاتف محمول قريب. يحدث تخزين البيانات عادةً على جهاز (مثل الهاتف المحمول أو الحاسوب المحمول) أو على خادم أو في النظام السحابي.

سيتم إرسال البيانات التي تم جمعها أثناء الخطوات المختلفة لاستجابة المساعدات النقدية والقسائم (تقييم الاحتياجات والاستهداف والتسجيل والتسليم والتغذية الراجعة والمراقبة والتقييم والمساءلة والتعلم) بطرق مختلفة بالاعتماد على كيفية تصميم عملية جمع البيانات الخاصة بك. يمكن أن تكون البيانات معرضة للخطر أثناء النقل والتخزين لأسباب مختلفة، لذلك من المهم أن تقوم بنقل البيانات وتخزينها بطرق آمنة تقيّد من يمكنه الوصول إليها. غالبًا ما يعمل ممارسو المساعدات النقدية والقسائم مع الشركاء وتطبيقات الجهات الخارجية وستحتاج إلى التأكد من أن البيانات التي تم جمعها من السكان المتأثرين ليست عرضة للوصول غير المصرح به أو التغيير أو الحذف أو المشاركة بطرق تؤدي إلى احتمالية حدوث ضرر، كما يمكن أن تساعد اتفاقيات نقل البيانات في إضفاء الطابع الرسمي على نقل البيانات بين الجهات الفاعلة في المساعدات النقدية والقسائم.

في الوثيقة الإرشادية 4 نستكشف كيفية تقليل المخاطر المرتبطة بنقل البيانات وتخزينها.

اتبع توصيات أمن البيانات الأساسية لنقل وتخزين البيانات

يجب استخدام عدد من بروتوكولات أمن البيانات الأساسية من قبل أي شخص يقوم بجمع البيانات أو نقلها أو تخزينها، ويجب أن يستعرض ممارسو المساعدات النقدية والقسائم أولاً وقبل كل شيء سياساتهم المؤسسية وإرشاداتهم بشأن أمن البيانات وضمان الامتثال لها بالإضافة إلى المعايير القانونية والتنظيمية وأفضل الممارسات الأخرى.

الصندوق 17: طرق حماية البيانات عند استخدام الأدوات والتطبيقات الرقمية

- تجنب إنشاء أدوات جديدة وتطبيقات مخصصة فقد تتطلب موارد مكثفة لضمان الأمن وإدارة الأمن والحفاظ عليه واختبار العيوب المحتملة
- لا تستخدم نظامًا أو أداة لمجرد أن شريكًا أو مؤسسة نظيرة أو ممول يطلبها واعمل مع فريق أمن تكنولوجيا المعلومات ومسؤول الخصوصية أولاً للتأكد من أنها آمنة
- قم بتخطيط الوقت والموارد الكافية لإجراء تقييمات أمنية على الأدوات والمنصات
- استخدم فقط شبكات الوايفاي الآمنة والخاصة أو اتصل عبر شبكة افتراضية خاصة
- قم بتشفير الأجهزة ونقل البيانات واستخدام تطبيقات الرسائل المشفرة مثل Signal
- استخدم المصادقة ثنائية العوامل
- قم بزيارة المواقع الآمنة فقط (تلك التي تستخدم https - وليس فقط http - في عناوينها)
- استخدم كلمات مرور قوية ولا تشارك كلمات المرور ولا تستخدم معلومات تسجيل دخول واحدة وكلمة مرور واحدة لعدة أشخاص
- استخدام أنظمة تنظيمية تم فحصها لنقل البيانات المشفرة وتخزينها (على سبيل المثال Microsoft SharePoint لنقل الملفات بدلاً من برامج مشاركة الملفات التابعة لجهات خارجية)
- استخدم متصفحات الخصوصية ومحركات البحث الأولى (Firefox و DuckDuckGo).
- حافظ على البرامج والحماية من الفيروسات محدثة

سيتمكن فريق أمن تكنولوجيا المعلومات الخاص بك من إرشادك بشأن أكثر الطرق أمانًا لنقل البيانات وتخزينها. قد تحتاج إلى العمل مع فرق تكنولوجيا المعلومات الخاصة بك على مستوى المقر الرئيسي لتحديد بعض التحديات السياقية بحيث يمكن إجراء مقايضات مدروسة في حال تعارض أمن البيانات مع سهولة العمليات مما يزيد من احتمالية تجاوز الأشخاص للأمان إلى تسهيل ممارسات العمل. إن هذا مجال رئيسي يجب تحديده في تقييم تأثيرات حماية البيانات أو تقييم المخاطر مقابل المنافع (نظر الوثيقة الإرشادية 2). قد لا يكون أمن البيانات على رأس اهتمامات الموظفين والباحثين خاصة في حالات التوتر الشديد والنزاع، حيث تميل التدابير الأمنية التقنية العليا إلى إبطاء الأنظمة والعمليات وقد يضطر الموظفون إلى إيجاد طرق للتغلب عليها لتسريع عملهم. من الأهمية بمكان أن تؤكد مؤسستك على أهمية اتباع الإجراءات الأمنية الإلزامية، وأن تبدأ حوارًا مع الموظفين والعاملين في التعداد لتصميم تدابير أمنية من المحتمل اتباعها ولا تثقل عبء العمل بشكل غير ضروري.

في حالات النزاع، قد لا تنجح حتى أفضل التدابير الأمنية لأن مسؤولي التعداد أو الموظفين يتعرضون للتهديد الجسدي من قبل أولئك الذين يرغبون في الوصول إلى متلقي المساعدات النقدية والقسائم أو بيانات أخرى. إن إيجاد طرق لهم لتخزين كميات محدودة فقط من البيانات على الأجهزة وتقليل جمع أي بيانات حساسة يمكن أن يساعد في تقليل المخاطر التي يتعرض لها الموظفون والسكان المتأثرون. تسمح العديد من أدوات جمع بيانات الهاتف المحمول بنقل البيانات على الفور إلى النظام السحابي عند الضغط على "إرسال" بحيث لا يتم تخزين البيانات على الجهاز وهذا يمكن أن يساعد في حماية مسؤولي التعداد وموظفي الخطوط الأمامية. في بعض السياقات المتقلبة، كان على المنظمات إخفاء معايير الاحتياجات والضعف عن مسؤولي التعداد كآلية أخرى للحماية، ويُعتقد أن اتخاذ القرارات بشأن الأهلية خارج البلد يحمي العاملين في الخطوط الأمامية من الإكراه والتهديدات من قبل المجموعات التي ترغب في التدخل في برامج المساعدات النقدية والقسائم أو الوصول إلى البيانات الخاصة بالسكان المتأثرين.

بالإضافة إلى الفوائد المذكورة أعلاه، يتيح التخزين السحابي الوصول إلى مستويات عالية من قوة الحوسبة والمرونة من حيث الموقع وتدفق البيانات وتوفير التكاليف للمؤسسات. من المهم ملاحظة أن التخزين السحابي له أيضاً عيوبه من حيث الخصوصية والأمان. تحدد اللجنة الدولية للصليب الأحمر تحديين رئيسيين تمثلهما الخدمات السحابية؛ ألا وهما: الافتقار إلى مراقبة البيانات؛ ونقص الشفافية حول كيفية معالجة الخدمات السحابية للبيانات، وهم يوصون بأن تولي الجهات الفاعلة الإنسانية اهتماماً خاصاً بالمخاطر المتعلقة بما يلي: الوصول إلى الخدمات السحابية من مواقع غير محمية أو غير آمنة، اعتراض المعلومات الحساسة، مصادقة ضعيفة، خروقات البيانات لمزود الخدمة السحابية، وإمكانية الوصول من قبل الحكومة وسلطات إنفاذ القانون. ستحتاج إلى تقييم هذه الأمور ومعالجتها من قبل فرق الأمن والخصوصية لديك من أجل تحديد أفضل السبل لإدارة البيانات بمسؤولية، وهناك تحدٍ إضافي يجب مراعاته وهو أن بعض البلدان تحظر نقل بيانات مواطنيها خارج الدولة، بما في ذلك إلى الخوادم السحابية المستضافة خارج الدولة.

يمكن العثور على مصادر أكثر تفصيلاً حول أمن البيانات المؤسسية وتطبيقات حماية الخصوصية في **قائمة التحقق من الأمان** هذه وفي الوثيقة الإرشادية من ELAN بشأن التشفير

يقدم مركز البيانات الإنسانية **إرشادات حول عمليات نقل البيانات** و **الأمن للعمليات المؤسسية**

تقدم اللجنة الدولية للصليب الأحمر **لمحة عامة عن أنواع البيانات التي يتم جمعها تلقائيًا** عند استخدام التطبيقات والبرامج الرقمية، ويجب أن يؤخذ هذا في الاعتبار عند إجراء DPIA أو PIA أو RBA

إذا كنت تفكر في تخزين البيانات في النظام السحابي؛ فلا تنس مراجعة قوانين البيانات الوطنية والتأكد من حماية البيانات في السحابة من خلال اتفاقيات مشاركة البيانات مع مقدمي خدمات الاستضافة السحابية. نصيحة: راجع الفصل 10 من **دليل حماية البيانات** الصادر عن اللجنة الدولية للصليب الأحمر للحصول على نبذة عامة كاملة عن استخدام التخزين السحابي

استخدام والحفاظ على الوصول القائم على الدور

هناك طريقة أخرى مهمة لإدارة البيانات بشكل مسؤول وهي التأكد من أن الأشخاص المصرح لهم فقط يمكنهم الوصول إلى البيانات. على سبيل المثال، قد لا تسمح المؤسسة للمديرين على مستوى المنطقة بالوصول إلى البيانات على المستوى العالمي، وقد لا يتمكن مسؤولي التعداد من الوصول إلى أي بيانات في النظام، وقد يُسمح لهم فقط بتحميل البيانات إلى النظام. قد يتمكن الشركاء في برنامج المساعدات النقدية والقسائم الكبير فقط من الوصول إلى البيانات التي قاموا بتحميلها ولكن ليس البيانات التي تقوم المنظمات الأخرى بتحميلها. يجب أن تعكس هذه الأذونات القائمة على الأدوار السلطة والمسؤوليات فيما يتعلق بالبيانات المعنية، أي يجب أن تسمح فقط بالوصول إلى البيانات التي يحتاجها الأفراد المختلفون تماماً لأداء وظائفهم - لا أكثر ولا أقل. يجب إجراء مراجعات منتظمة لمراقبة مستويات الوصول إلى البيانات للأفراد أثناء انتقالهم إلى مناصب مختلفة داخل المنظمة أو مغادرتها، بالإضافة إلى وصول المستشارين والجهات الخارجية.

يمكن تعيين التصريح المتضمنة داخل أنظمة إدارة البيانات وهي طلبات يتم إجراؤها للوصول إلى بعض البيانات المقيدة. تتضمن آليات الأمن هذه التعيينات الزمنية وطلبات التنزيل وتتبع المشاهدة وأنواع أخرى من تتبع من يقوم بماذا داخل قاعدة البيانات، حيث يساعد ذلك فريق تكنولوجيا المعلومات أو مدير الأنظمة على المراقبة المستمرة لأمن قاعدة البيانات والوصول إلى البيانات. يمكن أن يساعدك هذا أيضاً في تحديد ما إذا كان قد تم اختراق سلامة البيانات أو إذا تم تنفيذ أي نوع من الاحتيال أو الخرق. يمكن أن تكون استضافة البيانات في النظام السحابي أكثر أمانًا في بعض الحالات حيث يتيح ذلك لأجهزة الكمبيوتر المحمولة والأجهزة الأخرى المعرضة للسرقة أو القرصنة أن تكون خالية من أي بيانات شخصية وحساسة.

تقلل مستويات الوصول المصرح به من إمكانية التغيير غير المصرح به للبيانات وتسرب البيانات وخرقها، ومع ذلك قد يكون الأمر محبطًا للمؤسسات التي تغذي البيانات في نظام أكبر إذا لم تتمكن من الوصول إلى الصورة الأكبر من خلال رؤية جميع البيانات. قد يبدو أن الوكالات الأكبر حجمًا تتحكم بعد ذلك في البيانات والقوة في الاستجابة لأن لديهم إمكانية الوصول إلى جميع البيانات من جميع الشركاء وبالتالي لديهم المزيد من المعرفة بشأن الاتجاهات والتي يمكن أن تساعدهم في طلبات التمويل والشراكات الأخرى. قد يكون من الجيد مناقشة هذه الأنواع من المواقف داخل الاتحادات أو مجموعة العمل النقدي للتوصل إلى حل عملي.

يجب على المؤسسات داخلياً إصدار تعليمات لفرق الموارد البشرية لوضع اتفاقيات حماية البيانات والسرية للأفراد الذين يمكنهم الوصول إلى البيانات للتوقيع عليها بحيث يكونوا مسؤولين عن المشاركة غير المصرح بها أو إتلاف أو إساءة استخدام البيانات.

5 الوثيقة الإرشادية

تحليل واستخدام البيانات

بمجرد توفر البيانات سواء كانت بيانات جديدة تم جمعها لاستجابة المساعدات النقدية والقسائم أو بيانات من المصادر الحالية؛ يجب مراجعتها للتأكد من جودتها وسهولة استخدامها. ستحتاج إلى مراجعة عمليات تحليل البيانات للتأكد من أن البيانات شاملة وأن تحليل البيانات لا يؤدي إلى استبعاد بعض الأفراد أو المجموعات من المزايا التي هم مؤهلون لها. إذا كنت تستخدم البيانات لاتخاذ قرارات آلية فمن المهم أن تكون معايير وعمليات اتخاذ القرار واضحة وشفافة بحيث يمكن مراجعتها من قبل جهات خارجية للتحقق من التحيز إذا كانت هناك شكوك أو ادعاءات بأن الفوائد يتم تخصيصها بشكل غير عادل. بالإضافة إلى ذلك يجب استخدام البيانات فقط للأغراض المخصصة التي تم جمعها من أجلها والتي من أجلها توجد موافقة أو أي أساس قانوني آخر لاستخدامها.

استخدم البيانات فقط للغاية التي تم جمعها من أجلها ما لم يتم الحصول على تصاريح جديدة

كما هو موضح في الوثيقة الإرشادية 2 (انظر الصندوقين 12 و 13 بشأن الأساس القانوني)؛ يجب أن يكون هناك أساس قانوني وغرض مشروع لمعالجة البيانات. قبل البدء في تحليل أو استخدام البيانات، راجع الأساس القانوني الذي تم بموجبه جمع البيانات في البداية وحدد (جنبًا إلى جنب مع فريقكالقانوني ومسؤول حماية البيانات) ما إذا كنت قادرًا على معالجتها بشكل قانوني.

غالبًا ما تتلقى المنظمات الإنسانية قوائم المشاركين في البرنامج لبرامج المساعدات النقدية والقسائم أو إحالات من مجموعات أخرى (مثل الشركاء المحليين أو الوكالات الزميلة أو هيئات الأمم المتحدة أو الحكومات). إذا تم جمع البيانات بموجب المصلحة القانونية والمهمة العامة / المصلحة العامة، فقد يكون من الجيد معالجتها إذا كانت المعالجة الثانوية على غرار ما تم إخبار الأشخاص به في الأصل حول كيفية استخدام بياناتهم. إذا تم جمع البيانات بموجب أساس الموافقة فستحتاج على الأرجح إلى الحصول على موافقة جديدة قبل استخدامها لغرض ثانوي. من المهم إشراك مسؤول الخصوصية أو الفريق القانوني للتأكد من أنك لا تنتهك القانون عند إعادة استخدام البيانات.

قد يرغب مقدمو الخدمات المالية وشركات شبكات الهاتف المحمول أو كيانات القطاع الخاص الأخرى بمراجعة قوائم المستفيدين أو الاحتفاظ بالبيانات الوصفية للأغراض القانونية والتي قد يكون مسموحاً بها بموجب متطلبات الامتثال القانوني

تغطي الوثيقة الإرشادية 5 الجوانب التي يجب مراعاتها لتحليل البيانات واستخدامها بشكل مسؤول في إعداد برامج المساعدات النقدية والقسائم

قد يرغبون أيضاً بتحديد المستفيدين من حيث الجدارة الائتمانية والتي قد لا تتوافق مع الغرض الأصلي من جمع البيانات (تقديم المساعدات النقدية والقسائم) وتتطلب أساسًا قانونيًا جديدًا لمعالجة البيانات وربما علاقة جديدة مع المستفيدين بموافقة جديدة أو إضافية أو أذونات أخرى. قد يكون إجراء هذا النوع من المعالجة غير قانوني وفقًا للنظام الأوروبي العام لحماية البيانات على سبيل المثال. يجب على المنظمات الإنسانية مراجعة أي معالجة بيانات إضافية من قبل مشغلي شبكات الهاتف المحمول أو مقدمي الخدمات المالية بحثًا عن ضرر محتمل قصير الأجل أو طويل الأجل يلحق بالسكان المتأثرين (على سبيل المثال عدم القدرة في المستقبل على الوصول إلى الائتمان أو تسويق منتجات الخدمات المالية الاستغلالية)، وقد يتعارض استخدام البيانات هذا مع المبادئ الإنسانية للحيادية والنزاهة والاستقلالية.

البيانات النظيفة والتحقق من جودتها

ستؤدي البيانات الفوضوية إلى نتائج منحرفة أو غير صالحة. سواء تم جمع البيانات مباشرة من قبل مؤسستك أو كنت تستخدم مجموعات البيانات أو القوائم التي يشاركها الآخرون؛ فإن تنظيف البيانات ضروري لضمان أن البيانات مفيدة، وقد يشمل ذلك التحقق من التكرارات والتحقق من معايير أهلية المشاركين والتحقق من جزء من القائمة. من المحتمل أيضًا أن تتضمن إزالة أي بيانات يمكن استخدامها لتحديد الأفراد في مجموعة البيانات ما لم تكن البيانات مطلوبة لتنفيذ البرنامج. تأكد من توثيق أي ثغرات وعيوب وقيود موجودة في مجموعة البيانات.

ملاحظة: كن حذرًا من عدم الكشف عن غير قصد عن بيانات أو معلومات إنسانية حساسة أثناء أو بعد التحليل و / أو التصور. يجب أن يتم تحليل البيانات الإنسانية الحساسة فقط في بيئة آمنة ومن قبل الأفراد المصرح لهم بالوصول إلى البيانات.

نصيحة: تقدم مبادرات IMPACT **إجراءات تشغيل قياسية** لتنظيف البيانات يمكنك استخدامه كدليل لعمليتك الخاصة.

حذف أو إلغاء تعريف البيانات الشخصية والحساسة من مجموعات البيانات حيثما أمكن

كما هو مذكور في الوثيقة الإرشادية 3؛ يعد تقليل البيانات بمثابة مبدأ أساسي لإدارة البيانات المسؤولة. تتمثل إحدى طرق تقليل كمية البيانات الشخصية أو الحساسة التي تحتفظ بها في إلغاء التعرف عليها، بمعنى آخر، إزالة معلومات التعريف بحيث تصبح البيانات "مجهولة". عندما تكون البيانات مجهولة المصدر أو مجهولة الهوية يتم إزالة الارتباط بين البيانات والأفراد الذين تتعلق بهم بحيث لا يمكن تحديد هوية الفرد في البيانات، ويتم ذلك عن طريق إزالة "المعرفات المباشرة" و "المعرفات غير المباشرة"، على سبيل المثال عن طريق إزالة رقم الهوية الوطنية أو تاريخ الميلاد، حيث تجعل هذه العملية البيانات أكثر خصوصية وتضع الأشخاص في خطر أقل لأنه تم حذفها من تحديد المعلومات أو تجميعها إلى مستوى لا يمكن فيه تحديد الأفراد.

من المهم أن تتذكر أنه حتى البيانات غير المعرّفة أو المجمعة يمكن أن تعرض مجموعات كاملة من الأشخاص للخطر - على سبيل المثال إذا كان من الممكن استخدام موقع مجموعات عرقية أو دينية معينة لمهاجمة تلك المجموعات. إذا تم نشر معلومات حول مكان حدوث توزيع المساعدات النقدية والقسائم فقد يؤدي ذلك إلى تدخل مجموعات غير مرغوب فيها أو إلحاق الأذى بالأفراد الذين يتلقون المساعدات النقدية والقسائم أو المنظمات التي توفرها. إلى جانب التخطيط أولاً لكيفية إخفاء الهوية أو إلغاء التعرف على البيانات الفردية؛ ستحتاج أيضاً إلى التفكير في كيفية حماية البيانات غير الشخصية، ويجب مشاركة بيانات معينة أو إصدارها فقط لمن يحتاجون إليها للأغراض المعتمدة وفي بيئات بيانات محمية بشكل مناسب مع ضوابط تقنية وتنظيمية مناسبة.

نظرًا لأن تحليلات التكنولوجيا والبيانات أصبحت أكثر تعقيدًا من أي وقت مضى؛ فستحتاج على الأرجح إلى دعم من بياناتك أو فريق تكنولوجيا المعلومات الخاص بك لإلغاء تعريف البيانات.

تعد البيانات المجهولة المصدر أكثر أماناً، ولكن إذا كانت عامة جدًا فإنها تصبح عديمة الفائدة لتقديم المساعدات النقدية والقسائم وستحتاج إلى إيجاد طرق لتقليل البيانات مع الاستمرار في تحقيق أهداف المساعدات النقدية والقسائم.

حتى إذا تم إلغاء تحديد البيانات على المستوى الفردي فقد تتم إعادة تحديد هوية الأفراد من خلال المطابقة (الإحصائية) مع مجموعات البيانات الأخرى أو ضمن نتائج المسح الفردية. غالبًا ما يتم دمج قوائم المساعدات النقدية والقسائم سواء داخل المؤسسات الفردية أو بعد مشاركة مجموعات البيانات. إذا كانت هذه هي الحالة، فسيصبح من السهل تحديد الأفراد ضمن مجموعات البيانات. يعد التحكم في الإفصاح الإحصائي إحدى الطرق لتقييم مخاطر إعادة تحديد الهوية وتقليصها قبل مشاركة البيانات، حيث يقدم مكتب تنسيق الشؤون الإنسانية إرشادات حول هذه الطريقة.

عند التعاون مع الشركاء التجاريين في المواقع التي توجد بها مخاوف بشأن خصوصية البيانات؛ قد يكون أحد الخيارات هو إبرام اتفاقية مع مقدم خدمة مالية واحد لاستخدام الحسابات الفرعية حيث يتم استكمال العناية الواجبة أو "اعرف عميلك" فقط على الوكالة المنفذة بصفتها صاحب الحساب الرئيسي وليس على من يدخلون إلى الحسابات الفرعية. يمكن الوصول إلى الحسابات الفرعية من خلال البطاقات الذكية (مثل بطاقات الدفع المسبق أو بطاقات الصراف الآلي) التي تحتوي فقط على أرقام مرجعية مرفقة بها ولا تتضمن تفاصيل شخصية. يستطيع متلقي النقد بعد ذلك سحب النقود دون مشاركة بياناتهم الشخصية مع مقدم الخدمات المالية، حيث تمتلك الوكالة المنفذة فقط المعلومات التي تربط البطاقة أو الحساب بمتلقي النقد.

صنع القرار المؤتمت

لقد حذر المقرر الخاص للأمم المتحدة المعني بالفقر المدقع وحقوق الإنسان في عام 2019 من أن إصلاحات الرفاهية التي تيسرها وتبررها وتحميها التقنيات الرقمية الجديدة يمكن أن تعكس القيم والافتراضات التي لا تتماشى مع مبادئ حقوق الإنسان،[37] فعلى سبيل المثال يمكن استبعاد الأفراد عن طريق الخطأ من الفوائد عندما يتم اتخاذ القرارات عن طريق البرامج الآلية. بالإضافة إلى ذلك، يمكن وضع علامة على الأشخاص أو تصنيفهم بشكل دائم بطرق يمكن أن تؤدي إلى التمييز في المستقبل، فعلى سبيل المثال قد يتم وضع علامة دائمة على الشخص الذي حصل على مزايا بسبب وضعه كلاجئ خلال مرحلة معينة من حياته من خلال خوارزميات اتخاذ القرار على أنه خطر ائتماني. نظرًا لأن برامج المساعدات النقدية والقسائم أصبحت رقمية بشكل متزايد؛ فمن المهم أن تظل القيم الإنسانية في المقدمة وألا يتفاقم ضرر البيانات والاستبعاد بسبب الأدوات والتكنولوجيا الرقمية التي يدمجها ممثلو المساعدات النقدية والقسائم في برامجهم. قد يسمح اتخاذ القرار المؤتمت على أساس البيانات بنطاق أكبر واتخاذ قرارات أسرع ولكن هذا لا يزال في المراحل الأولى وقد يؤدي إلى الاستبعاد أو الأضرار المستقبلية.

يحتوي النظام الأوروبي العام لحماية البيانات أيضًا على مواد محددة تحمي الأفراد الذين تخضع بياناتهم لعملية صنع القرار الآلي التي لها آثار قانونية أو آثار مهمة مماثلة عليهم. يفرض النظام العام لحماية البيانات على سبيل المثال أنه في حال إجراء هذا النوع من صنع القرار؛ فيجب أن يكون لدى الأفراد معلومات حول المعالجة ويجب أن تكون هناك طرق بسيطة لهم لطلب التدخل البشري أو الطعن في قرار ويجب عليك إجراء فحوصات منتظمة للتأكد من أن أنظمتك تعمل على النحو المنشود.

بينما معظم المؤسسات لا تستخدم صنع القرار المؤتمت في برامجها، إلا أنه يستخدم بشكل متزايد في القطاع التجاري للمعاملات المالية مثل الموافقات الائتمانية. في سياق المساعدات النقدية والقسائم تعمل بعض المنظمات على كيفية استخدام سجلات تفاصيل المكالمات لاستهداف المتلقين المحتملين للنقد.

في حالة استخدام صنع القرار المؤتمت يجب أن يكون في دعم عملية صنع القرار البشري وليس بدلاً منه. يجب أن تضمن منظمات المساعدات النقدية والقسائم أن أي عملية صنع قرار مؤتمتة تستخدم للاستهداف أو التسجيل يجب تنفيذها باستخدام خوارزميات مفتوحة وشفافة وبإشراف بشري وبحث مقارن واختبار للتحقق من التحيزات المحتملة وآليات واضحة للشكاوى والتعويض إذا كانت القرارات خاطئة أو تؤدي إلى ضرر في المستقبل.

راجع **دراسة الحالة** لشراكة التعلم النقدي **حول الاستهداف عن بعد باستخدام البيانات غير التقليدية** لمزيد من المناقشة حول هذا الموضوع.

37 ألستون، ب. (2019) "تقرير المقرر الخاص المعني بالفقر المدقع وحقوق الإنسان". الجمعية العامة للأمم المتحدة

6 الوثيقة الإرشادية

مشاركة البيانات

تعمل الجهات الفاعلة في المساعدات النقدية والقسائم في مجموعة متنوعة من السياقات بما في ذلك النزاعات النشطة وأزمات اللاجئين وحالات السكان النازحين داخلياً والحصار. تعد مشاركة البيانات ضرورية في إعداد برامج المساعدات النقدية والقسائم ومع مواءمة وتعاون مجموعات العمل النقدي والتحالفات، يتم إنشاء شراكات مع مقدمي الخدمات المالية ومشغلي شبكات الهاتف المحمول ويتم إنشاء روابط الحماية الاجتماعية ويتم مشاركة البيانات بشكل متكرر أكثر للتنسيق ولأسباب أخرى.

يدعم المانحون والجهات الفاعلة الإنسانية بشكل متزايد تطوير سجلات فردية أو اجتماعية لبرامج المساعدة الاجتماعية وزيادة قابلية التشغيل البيني ومشاركة المعلومات والابتعاد عن أنظمة المعلومات الإدارية المنفصلة وغير المتصلة. تضغط بعض وكالات الأمم المتحدة مثل برنامج الأغذية العالمي ومفوضية الأمم المتحدة لشؤون اللاجئين واليونيسيف ومكتب تنسيق الشؤون الإنسانية من أجل اتباع نهج مشتركة لمواجهة حالات الطوارئ الإنسانية والتعاون فيما بين الوكالات،[38] ومع ذلك غالبًا ما يتم تحديد فوائد مشاركة البيانات من حيث مكاسب الكفاءة ، مع القليل من الإشارة إلى الحماية والمزايا والمقايضات الأخرى.[39]

تحديد ما هي المعلومات التي تحتاج للمشاركة ومع من ولماذا

كما هو موضح في الوثيقة الإرشادية 2 الصندوق 10 بشأن مراقبي البيانات ومعالجي البيانات؛ يتخذ مراقبو البيانات قرارات حول كيفية جمع البيانات ومعالجتها. كما أنهم يتخذون قرارات بشأن مشاركة البيانات. لا ينبغي على معالجي البيانات اتخاذ قرارات بشأن من ولماذا يمكن مشاركة البيانات حيث يجب أن يكون هذا من اختصاص مراقب البيانات.[40]

قبل مشاركة أي بيانات، يجب تحديد المؤشرات التالية:

الغرض: لماذا تشارك؟ ما هي البيانات التي تشاركها؟ هل تحتاج إلى مشاركة كل ذلك لتحقيق الغرض أم يمكنك فقط مشاركة جزء منه أو في حقول معينة؟

القانونية: هل أنت قادر قانونياً على مشاركة هذه البيانات أو اتخاذ قرار بوجوب مشاركتها؟ هل لديك إذن و / أو تم إبلاغ السكان المتأثرين بأنه سيتم مشاركتها؟

تقدم الوثيقة الإرشادية 6 إرشادات حول مشاركة البيانات المسؤولة مع الاعتراف بأن هذا مجال مثير للجدل يحتاج إلى العمل على أساس كل حالة على حدة حسب السياق والجهات الفاعلة المعنية.

38 انظر هذا الإعلان المتعلق بنظام النقد المشترك
39 آر غودمان وآخرون 2020 مراجعة وتحليل أنظمة تحديد الهوية والتسجيل في الأزمات الممتدة والمتكررة
40 مكتب مفوض المعلومات في المملكة المتحدة (2018) "مسؤولو المراقبة والمعالجة"

- **الميكانيكا:** كيف ستشاركها؟ كيف سيتم تخزينها؟ هل قمت بفحص المؤسسة التي ستشارك البيانات معها للتأكد من قدرتها على الحفاظ على أمانها وخصوصيتها؟ (انظر الوثيقة الإرشادية 4 حول نقل البيانات وتخزينها)
- **الوصف:** هل قدمت وصفاً كافيًا للبيانات والسياق الذي تم جمعها فيه ومتى تم جمعها والمعلومات الرئيسية الأخرى بحيث لا يتم استخدام البيانات خارج السياق؟ [41]

ربما تحتاج إلى إنشاء إصدارات مختلفة من مجموعات البيانات لاستخدامات وشركاء مختلفين. لا يجب مشاركة البيانات الشخصية والحساسة إلا إذا كانت ضرورية للغاية وبعد إبرام اتفاقية مشاركة البيانات.

قبل مشاركة أي نوع من البيانات من الضروري أن تتأكد من أن الأشخاص المذكورين في البيانات يدركون ما سيحدث لبياناتهم وقد قدموا موافقتهم المستنيرة لاستخدامها أو أنه قد تم وضع أساس قانوني آخر لمعالجة البيانات ومشاركتها؛ هذا يعني أن المشاركين قد منحوا الإذن لمشاركة البيانات مع معرفة كاملة بالعواقب المحتملة (انظر الوثيقة الإرشادية 2والصندوقين 12 و 13).

يجب أن يكون الوصول إلى البيانات الشخصية والحساسة على أساس "الحاجة إلى المعرفة" وليس الأساس الافتراضي.

ضع في اعتبارك نوع شركاء الوصول الذين تحتاج لهم وإذا أمكن قم بتعيين تصاريح الوصول وتتبع قواعد البيانات للتحكم في من يمكنه عرض البيانات أو إضافتها أو تعديلها أو تنزيلها أو حذفها.

تقييم المخاطر والمنافع قبل مشاركة البيانات مع الحكومات

هناك افتراض شائع بأن أنظمة الحماية الاجتماعية الإنسانية المركزية ستشكل الأساس لأنظمة الحماية الاجتماعية طويلة الأجل أو التي تقودها الحكومة. يجب موازنة هذه الافتراضات مع جوانب الخصوصية وحماية البيانات بسبب الآثار المحتملة على الحقوق الأساسية للمستفيدين.[42] في بعض الحالات قد يكون نظام واحد هو الخيار الصحيح وفي حالات أخرى قد يعني سياق البلد والاستجابة أن هذا ليس مثالياً. في أي سياق يجب على المنظمات محاولة تقييم هذا بشكل مشترك لإيجاد أفضل حل للسكان المتأثرين من الأزمة.

يمكن أن ينطوي تبادل البيانات مع الحكومات حسب السياق على مخاطر عالية للسكان المعرضين للخطر؛ على سبيل المثال إذا تمت مشاركة بيانات المهاجرين غير النظاميين مع الحكومات التي لا ترحب بالمهاجرين أو تم الوصول إلى البيانات من اللاجئين أو السكان النازحين داخلياً من قبل الجماعات المسلحة المحلية التي ترغب في إلحاق الضرر بهم. بالإضافة إلى مشاركة البيانات القانونية (التي قد تكون ضارة) تحدث مشاركة البيانات القسرية على مستويات مختلفة من الاستجابة بما في ذلك على المستوى المحلي عندما يتعرض مسؤولي التعداد للتهديد والمضايقة، وفي المستويات الأعلى حيث تشعر الوكالات بالضغط لمشاركة البيانات من أجل أن يُسمح لهم بالعمل في بلد أو منطقة معينة من بلد ما. من المهم أيضاً أن تتذكر أن البيانات التي تتم مشاركتها مع جزء من الحكومة قد تتم مشاركتها بشكل أكبر مع جزء آخر من الحكومة وأن البيانات التي تتم مشاركتها مع الكيانات المكلفة بمشاركتها مع الحكومات قد تكون ملزمة بمشاركة البيانات التي تقوم بجمعها فيما بعد.

تذكر أن الحكومات تتغير وبالتالي فإن مشاركة البيانات التي قد تبدو غير إشكالية اليوم قد لا تكون كذلك في العام المقبل. لهذا السبب يعد تقليل البيانات والمشاركة المحدودة للبيانات من أفضل الممارسات كما هو مذكور في الوثيقة الإرشادية 2 حيث نتحدث عن إدارة البيانات. يجب أن يكون التغيير في الحكومة بمثابة حافز لمراجعة تقييم تأثيرات حماية البياناتالخاص بك وتحديثه.

انظر **دراسة حالة** شراكة التعلم النقدي **حول تبادل البيانات مع الحكومات.**

تقييم مخاطر ومنافع مشاركة البيانات والتعاون مع ائتلاف أو مجموعة العمل النقدي

يمكن لمشاركة البيانات واستخدام أنظمة مشتركة وقابلة للتشغيل المتبادل إذا تم إجراؤها بشكل جيد ومع الاهتمام الكافي بحماية البيانات، تسهيل عملية تنفيذ المساعدات النقدية والقسائم وتقليل الازدواجية والاحتيال. يوصى بإنشاء بروتوكولات مشاركة المعلومات على مستوى الاستجابة (عبر ICCM أو HCT)، على سبيل المثال في التوجيه التشغيلي للجنة الدائمة المشتركة بين الوكالات بشأن مسؤولية البيانات. يوصى أيضًا بإنشاء بروتوكولات مشاركة المعلومات الخاص بمجموعة العمل النقدي في السياقات التي يكون فيها هذا مفيداً. في الوقت نفسه نظراً لأن البيانات هي القوة فغالبًا ما تكون هناك تحديات داخل الاتحادات أو مجموعات عمل المجتمعات عند تحديد النظام الذي يجب استخدامه ومن يصل إلى البيانات ويديرها داخل النظام. بالإضافة إلى ذلك يمكن للأنظمة الفردية وزيادة مشاركة البيانات أن تعرض بيانات متلقي المساعدات النقدية والقسائم لانتهاكات الخصوصية بالإضافة إلى الضرر المباشر في حالة انتهاك البيانات أو مشاركتها مع الجهات الفاعلة التي تسيء استخدامها.

41 ايه دورنوبس 2020 مشاركة البيانات مع الشركاء
42 آر غودمان وآخرون 2020 مراجعة وتحليل أنظمة تحديد الهوية والتسجيل في الأزمات الممتدة والمتكررة

غالبًا ما يواجه أعضاء الائتلافات و / أو أعضاء مجموعة العمل النقدي تحديات في التعاون ومشاركة البيانات مع بعضهم البعض. كما هو مذكور في الوثيقة الإرشادية 1 حول السياق والقدرات عملية تحديد من يقود الاستجابة ومن يشارك البيانات مع من هو محفوف بالتوترات المتعلقة بالسلطة والتحكم في الاستجابة والوصول الحالي والمستقبلي إلى تمويل المانحين والنهج والمخاوف المختلفة فيما يتعلق بخصوصية مستلمي المساعدات النقدية والقسائم. تعرب بعض المؤسسات عن تحفظات حول مقدار البيانات التي يتم التقاطها من متلقي المساعدات النقدية والقسائم وما إذا كان ذلك يتضمن القياسات الحيوية وما إذا كانت أنظمة البيانات التي يديرها ممثلون آخرون آمنة بدرجة كافية. علاوة على ذلك قد يتعين على الشركاء المنفذين الذين تمولهم الأمم المتحدة مشاركة البيانات مع وكالات الأمم المتحدة من أجل المشاركة في الاستجابة. من الواضح أن التوترات تحدث عندما يعتمد توفير التمويل على ترتيبات مشاركة البيانات لأن توفير البيانات والوصول إليها والتحكم فيها أمر سياسي وينطوي على ديناميكيات السلطة.

بينما سيكون لكل مؤسسة أنظمتها الخاصة؛ إذا كانت مشاركة البيانات جزءًا من استجابة المساعدات النقدية والقسائم فستحتاج البيانات إلى أن تكون قابلة للتشغيل البيني بحيث يمكن أن تغذي نفس نظام إدارة المعلومات، وهذا جانب آخر من التحديات في مشاركة البيانات؛ ألا وهو الاتفاق على البيانات التي ينبغي جمعها وكيف ينبغي تنظيمها بحيث يمكن استخدامها بفعالية.

تبتكر بعض الجهات الفاعلة في المساعدات النقدية والقسائم والائتلافات ومجموعات العمل النقدي بطرق مختلفة لمشاركة البيانات ضمن اتفاقيات مشاركة البيانات المعمول بها. على سبيل المثال إذا لم يكن لدى المؤسسات اتفاقيات مشاركة البيانات مع بعضها البعض ولكن لكل منها اتفاقية مشاركة بيانات مع وكالة ثالثة فقد يقررون مشاركة البيانات مع الوكالة الثالثة والتي يمكن أن تكون بعد ذلك بمثابة رابط مع البقاء ضمن الاتفاقيات القانونية واتفاقيات مشاركة البيانات. يقوم أعضاء مجموعات العمل النقدي الآخرين بتجربة طرق مختلفة لمشاركة البيانات بشكل مجهول الهوية، على سبيل المثال من خلال "تجزئة" آمنة أو استخدام blockchain. طور برنامج شبكة الأمان الاجتماعي في حالات الطوارئ في تركيا بنية معلومات مشتركة للبيانات عبر الشركاء ولمواءمة أنظمة المعلومات دون مشاركة البيانات مع جميع الجهات الفاعلة، حيث يمكن للجهات الفاعلة في المساعدات النقدية والقسائم أيضًا إنشاء بروتوكولات مشاركة المعلومات أو إجراءات التشغيل القياسية التي توجه كيفية مشاركة البيانات بين الوكالات أو فيما بينها.

يمكن استخدام قانون حماية البيانات لاتخاذ مزيد من القرارات حول إدارة البيانات. يتحمل مراقبو البيانات المسؤولية في حالة وجود خروقات للبيانات أو انتهاكات أخرى للخصوصية ويكون المراقب مسؤولاً عن إدارة أي طلبات متعلقة بالمساءلة من السكان المتضررين. من خلال تحديد من هو مراقب البيانات ومن هو معالج البيانات أو إذا كان سيكون هناك وحدات مراقبة مشتركة قد تتمكن المؤسسات من إيجاد أرضية محايدة لإجراء مناقشة مفتوحة تتعلق بالسلطة والمساءلة (انظر الوثيقة الإرشادية 2 الصناديق 10 و 11 بشأن مراقبي ومعالجات البيانات).

استعراض سياسات بيانات مقدمي الخدمات المالية ولأطراف الثالثة قبل الموافقة على مشاركة البيانات

مع تحول طرائق النقد لتشمل المزيد من مقدمي الخدمات المالية وشركات تشغيل شبكات المحمول؛ تشارك الجهات الفاعلة في المساعدات النقدية والقسائم البيانات الشخصية للمشاركين في البرنامج بشكل متكرر مع مقدمي الخدمات المالية وحكومات البلدان المضيفة لتلبية متطلبات اعرف عميلك ومتطلبات أخرى. قد تتضمن هذه البيانات الأسماء أو أرقام الهواتف أو أرقام الهوية بالإضافة إلى البيانات البيومترية بشكل متزايد. غالبًا ما يحتفظ مقدمو الخدمات المالية بسجلات معاملات بالإضافة إلى البيانات الشخصية، حيث توفر هذه السجلات مكان ووقت قيام الأشخاص بإجراء عمليات الشراء ومعلومات حول المدخرات والإنفاق. يجب حماية بيانات المعاملة هذه من سوء الاستخدام. من المهم للجهات الفاعلة في المساعدات النقدية والقسائم أن يكون لديها صورة واضحة عن البيانات التي سيجمعها مقدمو الخدمات المالية حول المشاركين في البرنامج أثناء تقديم خدماتهم وتقييم المخاطر المحتملة التي يمكن أن يشكلها ذلك على السكان المتضررين أثناء عملية تقييم تأثيرات حماية البيانات أو تقييم المنافع مقابل المخاطر. يجب أن تكون هناك شروط واضحة لمشاركة البيانات في أي عقود بالإضافة إلى شروط تتعلق بالمسؤولية عن أي نوع من تسريب البيانات أو خرقها.

عند إعداد اتفاقيات لمشاركة البيانات مع شركاء القطاع الخاص بما في ذلك مقدمي الخدمات المالية وشركات تشغيل شبكات الهاتف المحمول، تأكد من مراجعة سياسات وأحكام وشروط مشاركة البيانات الخاصة بهم وتضمين شروطًا قوية في اتفاقيتك الخاصة لضمان المعيار المناسب لحماية البيانات ومسؤولية البيانات بشكل أكبر على نطاق واسع، بما في ذلك القيود المفروضة على المشاركة المستقبلية والاستخدام والاحتفاظ والإتلاف. قد يقوم البعض بتضمين بند افتراضي في عقودهم، مما يسمح "بالمشاركة مع طرف ثالث"، ما يعني أنه يمكنهم مشاركة أي بيانات مع أي شخص في المستقبل، ومن المحتمل أيضًا أن يكون لدى هؤلاء المزودين بند ينص على أنه إذا تم الحصول عليها أو بيعها، فإن أي بيانات يحتفظون بها ستكون جزءًا رئيسيًا من الأصول التي سيتم تضمينها في البيع أو الاستحواذ.

إذا لم تكن راضيًا عن هذا السيناريو، فتأكد من إثارة المسألة مسبقًا لمشاركة البيانات أو الاتفاق على شراكة. قد يكون من المعقول تماماً التراجع عن سياسة مشاركة البيانات الافتراضية وجعل الوصول إلى بيانات برنامج المساعدات النقدية والقسائم أكثر مراعاة وتخصيصًا للاحتياجات الخاصة للطرف الثالث.

يجب إجراء تقييمات العناية الواجبة على شركاء القطاع الخاص قبل مشاركة أي بيانات.
قد يتراجع مقدمو الخدمات المالية والأطراف الثالثة عن القيود المتعلقة بمشاركة البيانات واستخدامها مرة أخرى. في بعض الحالات قد يكون لديهم أسباب مشروعة (على سبيل المثال إذا كانوا بحاجة قانونيًا إلى تقديم بيانات "اعرف عميلك" أو غيرها من البيانات إلى الحكومات)

في حالات أخرى قد يكون لديهم نموذج عمل يعتمد على الاستفادة من البيانات وقد يكون هذا غير متوافق مع المهمة الإنسانية. في حين أن المتطلبات القانونية مثل "اعرف عميلك" غير قابلة للتفاوض، فمن الممكن إضافة بنود تحظر استخدام بيانات متلقي المساعدات النقدية والقسائم لأغراض تسويقية أو تنص على أن مقدمي الخدمات المالية يجب أن يكونوا شفافين ويجب عليهم إخطار المؤسسات عند وجود طلب لمشاركة البيانات مع السلطات الحكومية.

قد لا تكون الوكالات الزميلة على دراية بمخاطر مشاركة البيانات، لذلك من المهم إجراء مناقشة حول هذا الأمر قبل توقيع اتفاقيات مشاركة البيانات.

إنشاء اتفاقيات مشاركة البيانات قبل مشاركة أية بيانات

قبل مشاركة البيانات من المهم الإشارة صراحةً إلى نوع الأشياء التي يمكن أو لا يمكن إجراؤها باستخدام البيانات، حيث يتم ذلك عادة من خلال اتفاقية مشاركة البيانات. لا تحتوي اتفاقيات مشاركة البيانات بالضرورة على معلومات خاصة ببيانات البرنامج التي ستجمعها. وبدلاً من ذلك فإنهم يوضحون "ما يجب عمله وما يجب تجنبه" الذي قد ينشأ عند مشاركة البيانات، حيث يجب أن تتضمن المعايير الدنيا لأمن البيانات والخصوصية وتحديد المسؤوليات والمسؤولية عن انتهاكات خصوصية البيانات والانتهاكات الأمنية أو إساءة استخدام البيانات أو إعادة المشاركة دون إذن.

قد يستغرق إنشاء اتفاقية مشاركة البيانات عدة أشهر، حتى إذا كانت هناك اختصاصات قائمة للتعاون بين المنظمات والوكالات، ويرجع ذلك جزئيًا إلى أن وضع معايير التشغيل البيني يستغرق وقتًا كما يرجع ذلك أيضًا إلى أن المنظمات والوكالات عادة ما تحتاج إلى إشراك فرقها القانونية وفرق حماية البيانات وفرق تكنولوجيا المعلومات، الأمر الذي قد يتطلب مشاركة على مستوى الدولة والمستوى العالمي للمنظمات الدولية. في حين كان هناك اتجاه لمشاركة البيانات دون وجود اتفاق؛ تجدر الإشارة إلى أن اتفاقيات مشاركة البيانات واتفاقيات نقل البيانات مطلوبة بموجب القانون بموجب النظام الأوروبي العام لحماية البيانات وأنظمة خصوصية البيانات الأخرى. في بعض الحالات أصبح التفاوض بشأن اتفاقيات مشاركة البيانات بمثابة ممارسة في السلطة من قبل المنظمات الأكبر على المنظمات الأصغر.

يجب تضمين المعلومات المتعلقة بمشاركة البيانات في طلبات الموافقة أو غيرها من المعلومات التي يتم توفيرها للسكان المتأثرين بحيث يتضح لهم ما يوافقون عليه أو ما سيحدث ببياناتهم. حتى إذا لم تستخدم "الموافقة" كأساس قانوني لجمع البيانات، يجب عليك إبلاغ الأشخاص بشفافية عن أي أطراف ستشارك بياناتهم معها.

في الحالات التي يلزم فيها تنفيذ استجابة عاجلة ولم يتم التوصل إلى اتفاقية مشاركة البيانات بعد، قد تحتاج إلى مشاركة كمية محدودة من البيانات بموجب مذكرة تفاهم مركزة ومحددة زمنيًا حتى تتمكن من متابعة الاستجابة. إن هذه مقايضة يجب أخذها بعين الاعتبار. هل من الأفضل مشاركة البيانات حتى تستمر الاستجابة أم أن المخاطرة عالية جدًا؟ في هذه الحالات، قد ترغب في استخدام تصميم برنامج المساعدات النقدية والقسائم الأقل ثقلًا في البيانات والذي يمكنك إدارته.

تعد اتفاقيات مشاركة البيانات بمثابة أداة مهمة لإدارة البيانات المسؤولة. ومع ذلك فمن الناحية العملية قد يكون من الصعب تنفيذ آليات المساءلة لهذه الاتفاقيات ما يعني أن هناك القليل من المراقبة لكيفية استخدام البيانات أو مشاركتها بشكل أكبر. لهذا السبب، من المهم الالتزام بمبادئ تقليل البيانات عند التحديد الدقيق للبيانات التي يجب مشاركتها ومع من.

يجب أن تكون مشاركة البيانات بين أعضاء مجموعة العمل النقدي والائتلافات والحكومات ومقدمي الخدمات المالية مجالًا رئيسيًا للتقييم عند إجراء تقييم تأثيرات حماية البيانات أو تقييم تأثير الحماية أو تقييم المنافع مقابل المخاطر في تقييمات السياق والقدرات المبكرة وأثناء تصميم البرنامج والتخطيط. يجب عليك أيضًا إجراء بحث في الخلفية للتأكد من مستويات حماية البيانات التي تعمل أثناء الاستجابات السابقة وأنظمة البيانات التي يتم اقتراحها من أجل استجابة مشتركة.

وضعت المفوضية السامية للأمم المتحدة لشؤون اللاجئين وبرنامج الأغذية العالمي مذكرة تفاهم لتبادل البيانات وهي متاحة **هنا.**

يغطي **دليل مسؤولية البيانات** التابع لمكتب تنسيق الشؤون الإنسانية موضوع مشاركة البيانات.

تحديد الاستراتيجية والتمرين على المنع والاستجابة لمشاركة البيانات القسرية وحوادث البيانات الحساسة الأخرى

بالإضافة إلى مشاركة البيانات المتفق عليها، في العديد من سياقات برامج المساعدات النقدية والقسائم، تعد "مشاركة البيانات القسرية" حقيقة واقعة. قد يتم إجبار موظفيك وشركائك المحليين بوسائل مختلفة على مشاركة البيانات مع المجموعات التي يمكنها الاستفادة من الوصول إلى البيانات والتحكم فيها. هناك أيضاً مخاوف من أن بعض الكيانات تشارك البيانات التي لا ينبغي مشاركتها، مثلاً عندما لا ترغب بعض المنظمات في مشاركة البيانات مع الحكومات ومع ذلك يتم الحصول على البيانات عبر مقدمي الخدمات المالية أو وكالة شريكة أخرى. من المهم تحديد مجالات المخاطر المحتملة للمشاركة القسرية للبيانات والتدرب على كيفية استجابتك أنت وموظفيك.

راجع الوثيقة الإرشادية 2 التصميم والتخطيط للمزيد من المعلومات حول حوادث البيانات الحرجة.

تشجع شراكة التعلم النقدي مجموعات العمل النقدي والائتلافات على التعاون ووضع استراتيجيات مشتركة حول كيفية الاستجابة لحوادث البيانات الشائعة في سياقاتها، والمساهمة في تسجيل هذه الحوادث بحيث يمكن إجراء المزيد من البحث والتعلم بشأن الممارسات الجيدة. راجع **مبادرة CaLP Critical Data Incident Management** للحصول على مزيد من المعلومات.

تفعيل اتفاقيات مشاركة البيانات الخاصة بك

إن صياغة اتفاقيات مشاركة البيانات شيء وضمان تنفيذها شيء آخر. يجب أن تضمن المنظمات أن يكون موظفيها وشركائها على دراية بما يتضمنه تبادل البيانات والاتفاقيات الأخرى ذات الصلة بالبيانات مع الجهات المانحة والحكومات ومقدمي الخدمات المالية حتى لا تشارك المنظمات أو تدير البيانات خارج هذه الاتفاقيات وبذلك يلتزم الشركاء بما تم الاتفاق عليه.

تستغرق اتفاقيات مشاركة البيانات قدرًا كبيرًا من الوقت والجهد، وقد يكون من الصعب تنفيذها. سوف تتطلب موافقات من الفرق القانونية ومكاتب حماية البيانات والتي يمكن أن تستلزم مراحل مراجعة كبيرة. من المهم تطوير اتفاقيات مشاركة البيانات كأحد مهامك الأولى في الاستجابة وتزويد هذه العملية بالموارد بحيث يتم توفير الموظفين والوقت اللازمين منذ البداية.

حدد وقتًا لمراجعة الاتفاقيات مع الشركاء ومناقشة توقعات إدارة البيانات وقيود مشاركة البيانات في وقت مبكر من العملية. قم بتوفير التدريب إذا لزم الأمر. قد تحتاج إلى توفير دعم القدرات أو موارد أخرى للشركاء إذا كانوا يحتاجون إلى مهارات أو معرفة أو أنظمة محسّنة من أجل تنفيذ متطلبات المشاركة الآمنة والمسؤولة للبيانات والوفاء بها.

7 الوثيقة الإرشادية

حفظ والاحتفاظ بالبيانات وإتلافها

ستحتاج البيانات التي تجمعها خلال دورة البرنامج إلى التخزين الآمن والمحافظة عليها بأمان كما هو مذكور في الوثيقة الإرشادية 4. عند إتمام الاستجابة يجب الاحتفاظ بالبيانات أو إتلافها بالاعتماد على الموقف، حيث يجب أن تحتفظ مؤسستك بالبيانات الشخصية والحساسة فقط طالما كان ذلك ضروريًا. بشكل عام كلما أسرعت في جعل البيانات الشخصية مجهولة المصدر أو مجمعة كان ذلك أفضل. بمجرد عدم الحاجة إلى البيانات لأغراض قانونية أو غيرها من الأغراض المشروعة يجب عليك إتلافها بشكل آمن.

تخطيط وإعداد ميزانية حفظ وحيازة وإتلاف البيانات منذ البداية

بينما يحدث الاحتفاظ بالبيانات وإتلافها في نهاية البرنامج أو نهاية دورة حياة البيانات، ستحتاج إلى التخطيط لذلك في المراحل الأولى من التصميم والتخطيط لضمان ميزانية كافية. يمكن أن يؤدي عدم التخطيط إلى تعريض المشاركين في البرنامج للخطر أو يتسبب في تخزين البيانات لفترة أطول من اللازم. من أجل التخطيط بشكل صحيح ستحتاج إلى فهم احتياجات جميع أصحاب المصلحة. حتى داخل البرنامج ذاته قد يكون للفرق المختلفة احتياجات مختلفة للاحتفاظ بالبيانات. على سبيل المثال قد يحتاج موظفو الشؤون المالية والامتثال إلى الوصول إلى بيانات البرنامج الخاصة بمراجعة الجهات المانحة بعد سنوات من انتهاء البرنامج. في المقابل، قد لا يحتاج موظفو البرنامج إلى البيانات بمجرد اكتمال البرنامج. لتلبية احتياجات البيانات لجميع الفرق من المهم الوصول إلى فهم مشترك لاحتياجات كل فريق للاحتفاظ بالبيانات قبل نهاية البرنامج وللتأكد من أن الأنظمة المستخدمة لجمع وتخزين بيانات البرنامج ستنسق بسلاسة من البداية إلى النهاية.

احتفظ فقط بالبيانات التي تحتاجها وبالتقسيمات التي تحتاجها وقم بإتلاف البقية

تجمع برامج المساعدات النقدية والقسائم الكثير من البيانات. اعتمادًا على نوع البرنامج وهيكلية التمويل قد تحتاج إلى الاحتفاظ بالبيانات ذات الصلة لتبرير اتخاذ القرار ولأغراض التدقيق أو لأغراض المراقبة والتقييم والتعلم. قد يخشى مديرو البرامج حذف البيانات خوفًا من حذف شيء مهم

توفر الوثيقة الإرشادية 7 إرشادات حول الاحتفاظ بالبيانات وإتلافها.

(توفر الوثيقة الإرشادية 4 المتعلقة بالنقل والتخزين مزيدًا من المعلومات حول تأمين البيانات للاستجابة النشطة).

وعلى الرغم من أن هذا قد يمثل مخاطرة؛ إلا أن الاحتفاظ بالبيانات لفترة طويلة يمثل مخاطرة أيضاً. كلما زادت البيانات الشخصية والحساسة التي يتم الاحتفاظ بها، زادت المسؤولية والمخاطر الأكبر التي تتحملها المؤسسة وزادت المخاطر التي يتعرض لها متلقو المساعدات النقدية والقسائم من احتمال تسرب بياناتهم أو الوصول إليها من قبل أولئك الذين قد يسيئون استخدامها أو يتسببون في إلحاق الضرر بهم. بالإضافة إلى ذلك مع مرور الوقت وتغيير الموظفين يصبح من الصعب بشكل متزايد ضمان دقة البيانات وإدراك الموظفين الجدد للقيود المفروضة على مجموعة بيانات معينة وإمكانية تتبع مصدر البيانات والتصاريح المرتبطة بها بدقة. علاوة على ذلك فإن المؤسسة التي تحتفظ بالبيانات هي المسؤولة عن تلك البيانات ويجب أن تكون قادرة على الاستجابة لطلبات المشاركين للوصول إلى بياناتهم الشخصية، فكلما زادت البيانات التي تحتفظ بها المؤسسة زادت صعوبة الأمر.

تستغرق اتفاقيات مشاركة البيانات قدرًا كبيرًا من الوقت والجهد، وقد يكون من الصعب تنفيذها. سوف تتطلب موافقات من الفرق القانونية ومكاتب حماية البيانات والتي يمكن أن تستلزم مراحل مراجعة كبيرة. من المهم تطوير اتفاقيات مشاركة البيانات كأحد مهامك الأولى في الاستجابة وتزويد هذه العملية بالموارد بحيث يتم توفير الموظفين والوقت اللازمين منذ البداية.

في حين أنه قد يكون من المغري الاحتفاظ بقوائم المستفيدين من المساعدات النقدية والقسائم لفترات طويلة، إلا أنها ستفقد أهميتها بعد فترة ولن تعود مفيدة لاستهداف النقد وتوزيعه إذا لم يتم صيانتها وتحديثها.

يشار إلى خطة الاحتفاظ بالبيانات أحيانًا باسم خطة الاحتفاظ والأرشفة والإتلاف. انظر ELAN

الوثيقة الإرشادية لمجموعة البيانات الأولية لمزيد من الإرشادات والأمثلة على RAD

www.calpnetwork.org

آذار 2021