إرشادات عملية لحماية البيانات في المساعدة النقدية والقسائم

ملحق لمجموعة أدوات النقد في حالات الطوارئ

يناير عام 2021

المحتويات

I. مقدمة 4

الجمهور المستهدف والغرض من الوثيقة 4

هيكل هذه الوثيقة 4

II. نظرة عامة على حماية البيانات 5

معالجة البيانات الشخصية 5

الأساس الشرعي 5

مبادئ حماية البيانات الرئيسية 5

III. الاستهداف 6

استخدام البيانات الشخصية 6

اعتبارات حماية البيانات 8

قرار المشروع 1: هل يجب علي استخدام بيانات المستفيد التي تم جمعها من قبل مصدر خارجي؟ 8

قرار المشروع 2: كيف يمكنني التحقق من أهلية المستفيدين؟ 9

قرار المشروع 3: هل يجب علي التحدث مع المستفيدين بشأن التعامل مع بياناتهم في هذه المرحلة؟ 11

IV. تسجيل المستفيدين 11

استخدام البيانات الشخصية 11

اعتبارات حماية البيانات 12

قرار المشروع 1: كيف يمكنني التحقق من هوية المستفيد؟ 12

قرار المشروع 2: ما هي البيانات الأخرى التي يجب أن أجمعها من المستفيدين أثناء التسجيل؟ 13

قرار المشروع 3: ماذا يجب أن اخبر المستفيدين عن كيفية إدارتهم لبياناتهم؟ 16

قرار المشروع 4: هل أطلب الموافقة من المستفيدين؟ 17

V. الاستعانة بمقدمي الخدمات المالية 19

استخدام البيانات الشخصية 19

اعتبارات حماية البيانات 19

قرار المشروع 1: هل يجب أن أستخدم مزود خدمات مالية؟ 20

قرار المشروع 2: ما هو نوع الحساب الذي يتعين اختياره من أجل توزيع المساعدة النقدية؟ 21

قرار المشروع 3: ما الذي يجب أن يتضمنه العقد المبرم مع مقدم الخدمات المالية؟ 22

VI. مشاركة البيانات مع الحكومات و المنضمات الإنسانية الأخرى و الجهات المانحة 23

استخدام البيانات الشخصية 23

اعتبارات حماية البيانات 24

قرار المشروع 1: أي من البيانات التي يجب مشاركتها مع الحكومة؟ 24

قرار المشروع 2: ما هي البيانات التي ينبغي مشاركتها مع المنظمات غير الحكومية الأخرى؟ 25

قرار المشروع 3: أي من البيانات التي يجب مشاركتها مع المانحين؟ 27

VII. رصد ما بعد التوزيع 27

استخدام البيانات الشخصية 27

اعتبارات حماية البيانات 28

قرار المشروع 1: ما هي البيانات الشخصية التي يجب أن أجمعها في عملية المراقبة؟ 28
قرار المشروع 2: ماهي بيانات المستفيدين التي يمكن لمقدمي الخدمات المالية أن يعطوها لي لكي أراقب البرنامج الخاص بي؟ 30
قرار المشروع 3: ماذا يمكن للتاجر إعطائي من بيانات المستفيدين في برنامج القسائم؟ 31
VIII. إرشادات عامة 32
اعتبارات حماية البيانات 32
تخزين البيانات 32
حفظ البيانات ومسحها 32
صلاحية الدخول 33
عملية الإرسال (مشاركة البيانات) 34
معالجة انتهاكات البيانات 35
إحاطة للموظفين والمتطوعين 35
تحليل ورصد مخاطر حماية البيانات 35
المشاركة المجتمعية والمساءلة 37
IX. مراجع 38

ا. مقدمة

بينما تنفذ الحركة الدولية للصليب الأحمر والهلال الأحمر التزاماتها لتوسيع نطاق المساعدة النقدية والقسائم، فإنها تعمل أيضًا على زيادة جمعها ومعالجتها للبيانات الشخصية، لا سيما تلك الخاصة بالمجتمعات الضعيفة التي يتم خدمتها. حماية البيانات ليست مجرد مسألة حكم جيد؛ إنما تتعلق أيضًا ببناء الثقة. قد يفكر المستفيدون خلال أوقات الأزمات في الأولويات الأكثر إلحاحاً والضرورية لبقائهم وسلامتهم من المخاطر التي تهدد بياناتهم الشخصية المقدمة لمنظمات المعونة. هذا هو السبب الأكبر الذي يجعل الممارسين في مجال النقد يحترمون بيانات المستفيدين ويكونون مسؤولين عنها. بالإضافة إلى ذلك، فإن أصحاب المصلحة الآخرين مثل الجهات المانحة والهيئات الحكومية والشركاء الآخرين سيزدادون ثقة في برامجنا للمساعدة النقدية والقسائم عندما تظهر معايير والممارسات الجيدة لحماية البيانات.

الجمهور المستهدف والغرض من الوثيقة

هذه الإرشادات العملية مخصصة **للممارسين في مجال النقد** أو أولئك الذين يديرون البرامج لإدراج مبادئ حماية البيانات أثناء تنفيذهم لبرامج المساعدة النقدية والقسائم. هناك العديد من المراجع المفيدة لحماية البيانات المتاحة للعاملين في المجال الإنساني، بما في ذلك دليل حماية البيانات في العمل الإنساني وسياسات حماية البيانات الخاصة بكل من الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر واللجنة الدولية للصليب الأحمر. في حين أن هذه المراجع تتسم بطابع أعم أو لا تتناول إلا بعض المسائل التي تواجه الممارسين في مجال النقد على مستوى عالٍ، فإن هذه الوثيقة تهدف إلى ترجمة المبادئ العامة لحماية البيانات إلى إرشادات عملية وقابلة للتطبيق، خاصة بالأنشطة الرئيسية في عملية المساعدة النقدية والقسائم. ستوفر هذه الإرشادات اعتبارات رئيسية بشأن حماية البيانات الممارسين في مجال النقد عند اتخاذ قراراتهم وتنفيذها.

تشير هذه الوثيقة إلى العمليات الموجودة في مجموعة أدوات النقد في حالات الطوارئ (CiE) وستكمل مجموعة الأدوات حتى تتم مراجعتها لتشمل مباشرة اعتبارات حماية البيانات الموضحة في هذه الوثيقة.

هام:
يتعين على الجمعيات الوطنية أن تضع هذه الإرشادات في سياقها الصحيح لتلبية المتطلبات التي تنفرد بها؛ وعلى وجه الخصوص، الالتزام بقوانينها وسياساتها الوطنية لحماية البيانات التي قد تكون أكثر صرامة من معايير حماية البيانات المطبقة هنا.

هيكل هذه الوثيقة

سيقدم القسم التالي نظرة عامة على حماية البيانات لتعريف القراء بالمبادئ والمصطلحات الأساسية التي سيتم استخدامها في الدليل. ثم سيتبعه فصول لكل عملية من العمليات الرئيسية الخمس الخاصة للمساعدة النقدية والقسائم.

قبل تطوير هذه الإرشادات، أُجري تحليل لمجموعة أدوات النقد في حالات الطوارئ لتحديد العمليات التي يتم فيها جمع البيانات الشخصية للمستفيدين ومعالجتها. ثم تم ترتيب أولويات العمليات استنادًا إلى مستوى معالجة البيانات الشخصية والمخاطر المحتملة. ستركز هذه الإرشادات على خمس من هذه العمليات ذات الأولوية[1]:

1. الاستهداف
2. تسجيل المستفيدين
3. الاستعانة بمقدمي الخدمات المالية
4. تبادل البيانات مع الحكومات والمنظمات الإنسانية الأخرى والجهات المانحة
5. رصد ما بعد التوزيع

سيحتوي كل فصل على نظرة عامة تصف كيفية استخدام البيانات الشخصية أو معالجتها بأمثلة تستند إلى مشاورات مع الجمعيات الوطنية. ثم تليها مجموعة من الاعتبارات المتعلقة بحماية البيانات استنادًا إلى القرارات أو الأسئلة الرئيسية المتعلقة بالمشاريع.

يبدأ كل اعتبار بمربع يسلط الضوء على قرار أو سؤال رئيسي بشأن المشروع. تشير أيقونة الجرس 🔔 إلى مبادئ حماية البيانات ذات الصلة بالاعتبار. بعد ذلك، يتم وضع إطار لمسألة المشروع ذات الصلة لإدراج اعتبار حماية البيانات. تُشرح تلك الاعتبارات بمزيد من التفصيل وترفق بأمثلة مبسطة لتوضيح كيفية تطبيق هذه الاعتبارات.

يتعلق الفصل الأخير بالاعتبارات العامة التي تنطبق على دورة برنامج المساعدة النقدية والقسائم بأكملها.

[1] تهدف هذه إلى أن تكون وثيقة فعّالة وإرشادًا عمليًا لمجالات أخرى من مجموعة أدوات النقد في حالات الطوارئ والتي يمكن تطويرها في مراجعات لاحقة كلما ازدادت خبرتنا في مجال حماية البيانات.

II. نظرة عامة على حماية البيانات

معالجة البيانات الشخصية

ما هي بالضبط البيانات الشخصية؟ **البيانات الشخصية** هي أي معلومات قد تؤدي إلى تحديد شخص طبيعي على قيد الحياة (موضوع البيانات). يمكن أن تكون البيانات شخصية حتى لو بدت للوهلة الأولى وكأنها غير مرتبطة مباشرة بشخص ما ولكن يمكن أن تؤدي إلى تحديد الهوية بشكل غير مباشر باستخدام معلومات إضافية. قد يبدو هذا معقداً، ولكنه يعني أساساً أن حماية البيانات تغطي مجموعة واسعة من المعلومات، وأن مصطلح "البيانات الشخصية" لا ينبغي أن يفسر تفسيراً ضيقاً. ستكون معظم البيانات التي ستجمعها من المستفيدين مؤهلة لأن تكون بيانات شخصية في سياق المساعدة النقدية والقسائم، على سبيل المثال:

- الأسماء وتفاصيل الاتصال
- أرقام الهوية
- أرقام الحسابات المصرفية
- تفاصيل العمل
- الوضع العائلي
- الحالة الصحية
- العنوان أو الموقع الجغرافي

بل على العكس من ذلك، فإن البيانات التي تجمعها لتحليل الموقف على **مستوى تجريدي** (على سبيل المثال، المعلومات الاقتصادية في المنطقة، وما إلى ذلك) لا تعتبر عادةً بيانات شخصية. هذه البيانات مجهولة المصدر، لأنها لا تتناول معلومات الأشخاص على الإطلاق، أو لأن المعلومات تكون في صيغة مجمعة. **البيانات المجمعة** هي البيانات التي يتم إنشاؤها عن طريق تلخيص ودمج البيانات الفردية. لا يمكن تحديد هوية الأفراد في البيانات المجمعة (لا بشكل مباشر ولا غير مباشر)، والتي تقدم عادةً نظرة عامة باستخدام المخططات والجداول والإحصائيات والمعلومات العامة عن مجموعات من الناس وليس عن الأفراد. تشمل الأمثلة إحصاءات عن أنواع سبل العيش، أو متوسط حجم الأسرة أو دخلها، أو نسب مئوية عن الأضرار التي تلحق بالمأوى داخل منطقة ما، أو حساب الحد الأدنى لسلة الإنفاق (MEB).

تعني **معالجة** البيانات الشخصية بشكل أساسي أي شيء تفعله بالبيانات، مثل جمعها وتخزينها وتنظيمها ومشاركتها وتقييمها وتعديلها ونشرها وتسجيلها واستخدامها وتصحيحها وحتى حذفها.

الأساس الشرعي

تتطلب معالجة جميع البيانات الشخصية أساسًا شرعيًا (أو *قانونيًا*). ثمة أساس شرعي شائع الاستخدام هو الموافقة. ومع ذلك، هناك العديد من الأسباب الأخرى للمعالجة المشروعة للبيانات الشخصية، بما في ذلك:

- الامتثال لالتزام قانوني
- تنفيذ عقد يتعلق بصاحب البيانات
- مهمة تصب في المصلحة العامة
- المصلحة (المصالح) الحيوية للشخص (تهديد على المدى القريب لصحته العقلية أو الجسدية)
- المصلحة المشروعة للجهة (يمكن أن يكون الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر، واللجنة الدولية للصليب الأحمر، وجمعية وطنية، على سبيل المثال) عبر معالجة البيانات الشخصية

أي أساس شرعي يمكن الاعتماد عليه يمكن أن يكون صعباً في بعض الأحيان. يمكن الاطلاع على مزيد من التفاصيل عن تعريف واختلاف هذه الأسس المشروعة في سياسة الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر بشأن حماية البيانات و دليل حماية البيانات في العمل الإنساني الذي أعدته اللجنة الدولية للصليب الأحمر ومركز الخصوصية في بروكسل.

ومن الشائع جدًا بالنسبة للمساعدة النقدية والقسائم الاعتماد على الموافقة. يقوم العديد من الممارسين في مجال النقد بتضمين سؤال الموافقة في بداية الاستبيان أو نموذج جمع البيانات. بيد أن هذا ليس بالضرورة الخيار الأفضل في حالات الطوارئ. يَرد شرح أكثر تفصيلًا لذلك في الفصل المتعلق بتسجيل المستفيدين الذي يتضمن أصل قرار للمساعدة على تقييم ما إذا كان أحد الأسس المشروعة الأخرى أكثر ملاءمة في ظل هذه الظروف.

مبادئ حماية البيانات الرئيسية

هناك عدة مبادئ لحماية البيانات يجب مراعاتها عند معالجة البيانات الشخصية. ورغم أن المسميات قد تتغير تبعًا للسياسة العامة أو الصك الدولي، فمن المقبول عمومًا أن المبادئ الرئيسية لحماية البيانات هي: (1) الشرعية والإنصاف والشفافية، (2.) تحديد الغرض؛ (3.) تقليص البيانات؛ (4) الدقة؛ (5.) تقييد التخزين؛ و (6.) النزاهة والسرية (الأمان). يمكنك أن تجد المزيد من التفاصيل حول ذلك في سياسة الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر بشأن حماية البيانات و دليل حماية البيانات في العمل الإنساني.

ولكن، من أجل أهداف هذا الدليل، سنقوم بالتركيز على المبادئ الأكثر ارتباطًا بالمساعدة النقدية والقسائم (مع ملاحظة أن مبدأ الشرعية، أو "الأساس الشرعي"، سبق مناقشته أعلاه). غالبًا ما تتم مناقشة المبادئ معًا حيث ينبغي النظر فيها بشكل مشترك لإجراء تحليل حماية البيانات الأكثر ارتباطًا، على الرغم من أنها تعتبر مبادئ جليّة بالمعنى الدقيق للكلمة. على سبيل المثال، نُناقش في القسم التالي مبدأين بارزين هما "تقليل البيانات إلى الحد الأدنى" و "تحديد الغرض" معًا، لأنه من غير الممكن تقييم البيانات الضرورية دون تقييم الغرض (الأغراض) من جمع / معالجة البيانات.

تقليص البيانات، الضرورة، تحديد الغرض

يُقصد بمبدأ تقليص البيانات: "جمع أقل ما يمكن وبقدر ما يلزم فقط." لتحديد ما هو ضروري، من المهم التحديد الواضح *للغرض* الذي ستستخدم البيانات المعنية من أجله. في سياق المساعدة النقدية والقسائم، قد تخدم معالجة البيانات الشخصية أغراضًا مختلفة (على سبيل المثال، التحقق من معايير الاستهداف، والتحقق من الهوية، وتسهيل التوزيع النقدي، واكتشاف أو تجنب الاحتيال، ومراقبة تأثير البرنامج). ينبغي أن تكون معالجة البيانات الشخصية *ضرورية* لتحقيق الغرض المحدد. من الضروري فهم ماهية المعلومات المطلوبة في السياق المحدد قبل القيام بجمع البيانات. إذا كنت غير متأكد من سبب قيامك بجمع مجموعة معينة من البيانات أو كنت تعتقد أنها قد تكون مفيدة لاحقًا دون مبرر منطقي محدد، أو كنت تعتقد ببساطة أنه كلما جمعت بيانات أكثر من المستفيدين كان ذلك أفضل، إذًا ربما ستجمع معلومات شخصية أكثر من *اللازم*. لتحديد البيانات اللازمة بوضوح، يُقترح مراجعة مبادئ تقليص البيانات / الضرورة / تحديد الغرض. تُعد هذه المشكلات أساسية لحماية البيانات وستطرح غالبًا في هذا الدليل. يتم توفير مزيد من التفاصيل والأمثلة ذات الصلة في فصل الاستهداف.

بالإضافة إلى ذلك، لا يمكن استخدام البيانات الشخصية التي تم جمعها لغرض محدد لأي غرض آخر. يمكن بالطبع استخدام مجموعة البيانات الحالية لأغراض مستقبلية في ظروف معينة. غير أن الأغراض المستقبلية يجب أن تكون عموماً "متوافقة" مع الغرض الأصلي. يكون هذا التوافق موجود عندما تكون الأهداف وثيقة الصلة، بحيث يمكن افتراض أن صاحب البيانات لن يفاجأ بهذا الاستخدام الثانوي. فعلى سبيل المثال، توفرت الأموال الإضافية في نهاية برنامج المساعدة النقدية والقسائم بحيث لم تكن متوقعة من قبل. ستُعتبر مراجعة بيانات المستفيدين التي تم جمعها مسبقًا لتحديد من يجب أن يتلقى مساعدة جديدة متوافقة مع الغرض والأساس القانوني الذي تم جمع البيانات الشخصية بناءً عليه مسبقًا. وبخلاف ذلك، لابد من تحديد أساس قانوني مناسب وقد يحتاج أصحاب البيانات إلى تلقي معلومات محدثة عن الاستخدام الإضافي المقصود (اطلع على مبدأ الشفافية التالي).

الشفافية

الشفافية تقترن بالإنصاف. الفكرة هي أن تكون صريحًا وصادقًا حول التعامل مع البيانات الشخصية. ووفقًا لمبدأ الشفافية، يجب أن يتلقى الأشخاص المعنيون بالبيانات دائمًا معلومات أساسية معينة حول ما يحدث لبياناتهم، بما في ذلك:

- حقيقة أنّ بياناتهم الشخصية تتم معالجتها والأساس الذي تقوم عليه هذه المعالجة
- من يقوم بمعالجة البيانات
- لأي غرض (أغراض) تتم معالجة البيانات
- كيف يتم تخزين البيانات وما هي مدة التخزين
- ما إذا كانت ستتم مشاركة بياناتهم مع أية جهة أخرى
- الحقوق التي يملكونها بخصوص معالجة بياناتهم، كحق تصحيح أو حذف البيانات
- معلومات الاتصال أو الشخص الذي ينبغي الرجوع إليه في حالة وجود أسئلة أو شكاوى لدى أصحاب البيانات

يختلف الشكل الذي تقدم به هذه المعلومات باختلاف السياق. ستطرح أمثلة محددة خلال هذا الدليل.

أمان البيانات (السرية، والنزاهة، والحد من التخزين)

يجب التعامل مع البيانات الشخصية بسرية وأمان. قد يكون هذا بديهيًا، ولكنه ليس من الواضح دائمًا ما الذي ينبغي فعله لضمان السرية. يتطلب قانون حماية البيانات (أو السياسة، عند الاقتضاء) تنفيذ تدابير أمنية مختلفة، مثل القيود المفروضة على الوصول والوقاية من فقدان البيانات. والهدف النهائي هو تجنب انتهاكات البيانات، أي *الوصول غير المصرح به إلى البيانات الشخصية أو تدميرها أو فقدانها أو تغييرها أو الكشف عنها*.

III. الاستهداف

استخدام البيانات الشخصية

يسترشد استهداف المساعدة النقدية بأهداف البرنامج استناداً إلى الاحتياجات المقدرة. ينسق البرنامج الأنشطة مع مستفيدين محددين باستخدام معايير استهداف محددة، تشمل عادةً مؤشرات اجتماعية - اقتصادية ومؤشرات الضعف. لمزيد من المعلومات، راجع القسم 3_3M من مجموعة أدوات النقد في الطوارئ.

الشكل 1: الخطوات في عملية تحديد الأهداف

تتضح الخطوات العامة في عملية تحديد الأهداف في *الشكل 1*. قد تعتمد هذه العملية على البيانات التي سبق جمعها للإبلاغ عن وضع المعايير وتسريع إنشاء القائمة الأولية للمستفيدين المؤهلين للحصول على المساعدة المقدمة من برنامج المساعدة النقدية والقسائم.

تتخذ الخطوات من 1 إلى 3 قرارات رئيسية في محاولة تحقيق أهداف البرنامج. تشمل هذه القرارات ما يلي:

- ما هي المواقع الجغرافية التي سيتم اختيارها للتدخل؟
- عمليات التوزيع الشاملة أم العشوائية؟
- إذا ما كان ينبغي التوجه نحو الأسر أو الأفراد؟
- ما هي معايير تحديد الأهداف التي ينبغي اختيارها استنادًا إلى عوامل الضعف، أو مدخلات اجتماعية - اقتصادية، أو مدخلات سياقية محددة؟
- ما هي آلية الاستهداف التي يتعين عليها أن تختار (آلية استهداف تصنيفية أو ذاتية أو مجتمعية)؟

بشكل عام، لا تؤدي البيانات الشخصية دورًا هامًا في الخطوات الثلاث الأولى. تستند القرارات إلى معلومات عامة أو بيانات مجمعة عن المناطق المتضررة والسكان ككل. لم يعد هنا الوضع الفردي للمستفيدين المحتملين موضع الاهتمام، بل الوضع العام على الأرض وأهداف البرنامج.

غير أن الخطوتين 4 و 5 تتناولان البيانات الشخصية حيث يجري تحليل المستفيدين المحتملين وفحصهم بالمقارنة مع المعايير التي تم تحديدها، ووضع قائمة أولية بالمستفيدين قبل عملية تسجيل المستفيدين الرسمية. ستتضمن القائمة أسماء المستفيدين على الأقل، وقد تنطوي عملية التحليل أو التحقق على معلومات مفصلة عن المستفيدين.

في الخطوة 4، يتم عادةً وضع القائمة الأولية على أساس آلية الاستهداف المحددة في الخطوة 3:

- **الاستهداف المجتمعي** – الأسر الضعيفة التي حددها قادة المجتمع وأفراده استنادًا إلى المعايير المتفق عليها؛ والنتائج التي حددتها الجمعية الوطنية وتحققت منها. على سبيل المثال، طلب قادة المجتمعات المحلية تحديد الأسر التي دمرت منازلها بالكامل.
- **الاستهداف الذاتي** - ويُطلب من الأفراد تقديم معلومات عن أنفسهم وتفاصيل تتعلق بالمعايير المتفق عليها. على سبيل المثال، يبحث فريق البرنامج عن متطوع بالغ غير مؤمن غذائيا يرغب في المشاركة في برنامج المساعدات النقدية عن طريق العمل.
- **التحديد الفئوي**- تستند الأهلية إلى فئات محددة من المستضعفين (على سبيل المثال ، الأسر التي يعيلها أطفال) ومن المحتمل سجل مدني جيد لتحديد الأفراد الذين ينتمون إلى فئة معينة للتحديد. على سبيل المثال ، يُطلب من مسؤولي الحكومة المحلية مشاركة قائمة أفراد المجتمع الذين يعيشون في فقر مدقع.

بغض النظر عن آلية التحديد المستخدمة ، تعتمد هذه الخطوة على البيانات المجمعة من مصادر مختلفة (على سبيل المثال ، الحكومة أو المجتمعات المحلية أو المنظمات الأخرى أو الأفراد). وعلى الرغم من أنه يمكن الحصول على القائمة الأولية من مصدر آخر، إلا أن حيازة القائمة يعتبر بالفعل استخدامًا للبيانات الشخصية. في صورة عدم توفر قائمة أولية، فقد تختار الجمعية الوطنية التوجه لاستراتيجية باب إلى باب في المجتمعات المتضررة لتطوير مثل هذه القائمات التي تطلب البيانات الشخصية.

في المرحلة الخامسة، يتم التحقق من أهلية كل الأشخاص المذكورين في القائمة الأولية. قد تشمل هذه العملية ممثلي المجتمع أو القادة المحليين الذين يعرفون السكان أو الذين قاموا بجمع المعلومات باستخدام بيانات أو أنظمة أخرى (على سبيل المثال ، السجل المدني أو قوائم الحماية الاجتماعية). في بعض الحالات ، قد تعتمد الجمعية الوطنية استراتيجية من باب إلى باب للتحقق مباشرة مع المستفيدين للتأكد من أنهم مؤهلون بالفعل بناءً على البيانات الشخصية التي يقدمونها. قد تتم عملية التحقق من الباب إلى الباب بالتوازي مع إنشاء القائمة الأولية وفق خطوة 4. قد تكون عملية التحقق هذه مشابهة لعملية تسجيل المستفيد وقد تستخدم نماذج الاستبيان وقاعدة بيانات لجمع البيانات الشخصية المنظمة وإدارتها أو يمكن أن تكون مخصصة باستخدام القلم والورق فقط لتحديد المعايير التي يستوفيها المستفيد -و يعتبر ذلك بيانات شخصية أيضا.

في نهاية عملية التحديد، يمكن مشاركة ونشر قائمة المستفيدين الذين تم التحقق منهم في المجتمع (على سبيل المثال ، يتم طباعة القائمة ونشرها في مساحة عامة للمجتمع المحلي للتحقق من المشمولين في المبادرة). يتم تصنيف نشر هذه القائمة على أنه استعمال (معالجة) للبيانات الشخصية، لأنك تجعل البيانات التي بحوزتك متاحة للآخرين - لجميع أعضاء المجتمع، حتى يتسن لهم تقييم القائمة.

اعتبارات حماية البيانات

ستشمل عملية التحديد معالجة البيانات الشخصية عند إعداد قائمة المستفيدين الأولية وعند التحقق من هذه القائمة كذلك. يتناول هذا القسم قرارات المشروع الأساسية في عملية التحديد واعتبارات تتعلق بحماية البيانات. المبدأ الأكثر أهمية الذي سيتعامل معه هذا القسم هو **تقليل استخدام البيانات / الحاجة لذلك.** تتعلق جميع المبادئ الأخرى بمعالجة البيانات التي جمعتها ، بينما يهدف تقليل استخدام البيانات والحاجة إليها إلى الحد من جمع البيانات في المقام الأول. إن عدم جمع البيانات التي لا تحتاجها للبرنامج هو الطريقة الأكثر فاعلية لتحسين مستوى حماية البيانات. وبالتالي، فمن الضروري التفكير في دورة حياة البرنامج وتحديد البيانات التي ستكون ضرورية مسبقًا خلال البرنامج، في مرحلة إعداد البرنامج وقبل جمع أي بيانات عن المستفيدين.

قرار المشروع 1: هل يجب علي استخدام بيانات المستفيد التي تم جمعها من قبل مصدر خارجي؟

تقليل استخدام البيانات، إلى أدنى حد والحاجة إلى ذلك وأمن البيانات

إعادة صياغة مشروع القرار: هل أحتاج إلى البيانات التي تم جمعها من قبل مصدر خارجي وكيف يمكنني التأكد من أن بيانات المستفيد قد تم جمعها بطريقة مناسبة؟

عند إنشاء قائمة المستفيدين الأولية، فمن الوارد استخدام بيانات المستفيدين من مصادر خارجية مثل المنظمات الأخرى أو الحكومة. لذلك ، قد يبدو سؤال قرار المشروع واضحًا وضروريًا. وعلى الرغم من ذلك، يستلزم سؤال قرار المشروع المعاد صياغته من الممارسين النقديين باتباع نهج دقيق لطلب واستخدام البيانات من المصادر الخارجية التي تضع في الاعتبار مبادئ تقليل البيانات وأمن البيانات ، لا سيما في حالة غياب اتفاقيات مشاركة بيانات ثابتة.

فيما يلي بعض الأمور الأساسية التي يجب اعتبارها عند التفكير في استخدام بيانات المستفيدين التي تم جمعها من قبل مصادر خارجية (المنظمات غير الحكومية الأخرى ، والحكومة ، وما إلى ذلك):

- **هل هذه المنظمة موثوقة وهل يمكنني الوثوق ببياناتها؟** إذا كانت المؤسسة التي تقدم البيانات غير معروفة، فقد ترغب في أن تسأل أو تتحقق من كيفية جمعها لبياناتها ، وهل تعتبر ذلك موثوقًا به أم لا؟ لا يكمن القلق هنا أن البيانات قد تكون غير كاملة أو غير صحيحة فقط ، ولكن في أنه قد تم الحصول على البيانات بشكل غير لائق أيضًا(على سبيل المثال ، عدم وجود أساس قانوني واضح أو عدم إبلاغ المستفيدين بكيفية مشاركة بياناتهم مع الآخرين خاصة إذا كانوا متحرجين و حساسين جدا). وفقا للسياق، قد يكون من المفيد سؤال قادة المجتمع أو المنظمات الأخرى الناشطة والفاعلة في المنطقة عما إذا كانوا يعرفون هذه المنظمة ويثقون بها. من المستحسن أيضًا أن تطلب من المنظمة تزويدك ببعض المعلومات عن الظروف التي جرت فيها عملية الجمع. من المهم معرفة ما إذا كان المستفيدون على دراية بإمكانية مشاركة بياناتهم معك. إذا كنت تشك في مصداقية إجراءات الجمع، فهذا مؤشر قد يدفعك في التفكير في مصادر البيانات الأخرى.

- **ما هي البيانات التي أطلبها وأوافق عليها؟** لا يمكن أن يعني سبب منظمة أخرى قد جمعت قدرًا معينًا أو نوعًا معينًا من البيانات، عليك حيازتها **برمتها أو معظمها**. مرة أخرى ، من الجيد التفكير في مبدأ تقليل استخدام البيانات والحاجة إليها. يعتمد ذلك على المشروع والبيانات التي يجب أن تطلبها أو تقبلها. إذا زودتك المؤسسة الأخرى ببيانات أكثر مما تحتاجه، فمن المستحسن أن تسأل فقط عن تلك البيانات وإذا تم توفير البيانات غير الضرورية، فاحذف تلك البيانات وأبلغ المؤسسة الأخرى، حتى يكونوا على علم بما تم الاحتفاظ به. يوصى بالحذر إذا كانت مجموعة البيانات قد تحتوي على فئات حساسة للغاية من البيانات، مثل المعلومات الصحية أو الجنسية أو الدينية، خاصة إذا كانت هذه البيانات لا ترتبط بصلة مباشرة باحتياجات برنامجك. قد يشير وجود منظمة توفر هذه الأنماط من البيانات بحرية مع أو بدون اتفاقيات مشاركة البيانات الرسمية إلى أن معايير حماية البيانات لديها ضعيفة أو منعدمة أصلا. علاوة على ذلك، ينبغي التعامل مع البيانات الواردة من جهات خارجية بمسؤولية.

لا يتضمن السيناريو الموضح أعلاه اتفاقيات مشاركة البيانات بين الأطراف، وبالتالي تصبح حيازة البيانات أحد الاعتبارات المهمة. بالنسبة لبرامج المساعدات النقدية و القسائم حيث تكون الجمعية الوطنية شريك منفذ لوكالة أخرى، يجب الاتفاق على تبادل البيانات بين الشركاء المعنيين، الخارجيين أو غيرهم، ويمكن تقييم هذه الاعتبارات عند التفاوض على اتفاقية مشاركة البيانات. إذا كنت قلقًا في سياق تلك البرامج النقدية بشأن حماية البيانات فيما يتعلق بمشاركة البيانات مع جهات خارجية، فيرجى إبلاغ مديرك أو الفريق القانوني داخل جمعيتك الوطنية ولاحظ المخاطر / المخاوف في مصفوفة مخاطر المساعدات النقدية و القسائم الخاصة بك .

أمثلة:

يتمثل المعيار المحدد في "الأسر التي لديها أطفال فقدوا منازلهم في الفيضان".

يقدّم فريق المجتمع الوطني طلبًا للحكومة المحلية لتوفير ما يلي:

- «معلومات ذات صلة» بالمقيمين في المنطقة. هذا الطلب واسع النطاق، ومن المحتمل أن تقدم الحكومة معلومات أكثر من اللازم. يجب تضييق نطاق هذا الطلب.

- «أسماء جميع المقيمين في المناطق المستهدفة وحالاتهم الاجتماعية». هذا الطلب أكثر تحديدًا، لكنه لا يزال واسع النطاق كثيرًا. الأشخاص الذين لا يملكون أطفالًا غير مستهدفين. لذلك من غير المحتمل أن يكون هناك حاجة لمعرفة أسمائهم.

- «فقط أسماء المقيمين في المناطق المستهدفة الذين يملكون أطفالًا». يمكن أن يكون هذا ضروريًا وكافيًا.

في المرحلة التالية من الزلزال سيحاول فريق المجتمع الوطني تحديد الأشخاص الذين فقدوا منازلهم. ستقدَّم إحدى الجمعيات في القرية الأكثر تضررًا معلومات تتضمن قوائم بالأشخاص الذين فقدوا منازلهم بسبب الزلزال. سيأخذ فريق المجتمع الوطني ذلك بعين الاعتبار. سيتواصلون مع محافظ القرية ويسألون عن سمعة الجمعية. كما سيتواصلون مع الجمعية بما يتعلق بعملية جمع البيانات التي يتبعونها. توضح الجمعية أنها قد أعلمت الناس بحماية البيانات وعن نية مشاركة البيانات مع المنظمات المساعدة الأخرى. تتضمن المعلومات التي جمعتها الجمعية: الأسماء، وحجم العائلات، وأعمار الأطفال، وأرقام الهواتف المحمولة. يخطط فريق المجتمع الوطني لتوزيع بطانيات لكافة العائلات التي خسرت منازلها. ثم يقررون أنه من أجل هذا التدخل فإنهم بحاجة فقط إلى أسماء المستفيدين وأرقام هواتفهم للاتصال بهم. يتأكد الفريق من عدم استلام بيانات أخرى غير تلك البيانات.

قرار المشروع 2: كيف يمكنني التحقق من أهلية المستفيدين؟

تقليل البيانات، الضرورة، السرية

إعادة صياغة مشروع القرار: أي البيانات التي سأحتاجها حقًا لتوثيق أهلية المستفيدين؟

هدف التحقق من أهلية المستفيدين هو معرفة ما إذا كان الشخص (أو العائلة) تلبي بالفعل معايير الاستهداف. هذا ما سيتم إنجازه في **الخطوة 5** من عملية الاستهداف المذكورة أعلاه حيث يمكن أن يكون من الضروري جمع أو تحليل البيانات ذات الصلة بالمستفيدين. عند إجراء هذا التحقق، من المهم عدم جمع أو معالجة بيانات أكثر مما هو مطلوب لإكمال المهمة (مبدأ تقليل البيانات والضرورة). يمكن استخدام طرق مختلفة للتحقق من الأهلية، وقد تتطلب أو تعالج البيانات الشخصية بشكل مختلف:

- **استخدام أعضاء المجتمع للتحقق.** في هذه الطريقة، قد لا يتم استشارة المستفيدين الفعليين مباشرة. بدلاً من ذلك، قد يقدم أفراد المجتمع الذين لديهم معرفة بالموقف أو التفاصيل الشخصية للمستفيدين قائمة أولية بالمستفيدين المؤهلين المحتملين. يمكن أن يتبع ذلك فحص تحقق أكثر رسمية أثناء عملية تسجيل المستفيد. عند استخدام هذه الطريقة، من المهم أن تكون خصوصية المستفيدين محمية، خاصة إذا كانت الطريقة تتم في مكان عام (أي مع أعضاء المجتمع الآخرين) وبما أن المستفيدين الفعليين لا يمكنهم الاعتراض على مشاركة المعلومات التي يعرفها الآخرون بالفعل معهم. يجب التقليل من الأسئلة التي يتم طرحها على قادة المجتمع حول البيانات الخاصة بالمستفيدين ويجب تجنب الأسئلة الحساسة في الأماكن العامة. إذا كانت أي معلومات يمكن عدّها معلومات حساسة ومطلوبة للبرنامج، فحاول فقط جمع هذه المعلومات في بيئة خاصة مثل التحقق ضمن المأوى.

- **التحقق ضمن المأوى.** قبل زيارة الأسر المستفيدة بالفعل للتحقق من أهليتها، من المهم تحديد البيانات الضرورية جداً لهذا الغرض، مع احترام مبدأ تقليل البيانات والضرورة مرة أخرى. نظرًا لكبر حجم الجهود المبذولة في التنقل للذهاب إلى المأوى، فقد يكون هناك ميل لطلب معلومات أكثر مما هو ضروري للغاية، وذلك لتجنب الاضطرار إلى تكرار الزيارة. لذلك، يعد التحضير لنطاق البرنامج والغرض منه أمرًا ضروريًا، بحيث لا يطلب سوى الحد الأدنى المطلق اللازم للتحقق. إذا لم تكن متأكدًا مما إذا كان يجب عليك طلب معلومات معينة، فاسأل نفسك السؤال التالي: ما هو تأثير المعلومات على قراري باستهداف المستفيد الفردي؟ إن لم تكن متأكدًا، فقد لا تكون تلك المعلومات ضرورية.

- **نشر قائمة المستفيدين الأولية.** كجزء من الخطوة 4 أو بعد الخطوة 5 في عملية الاستهداف الموضحة أعلاه، يتم عادةً مشاركة قائمة المستفيدين الأولية ونشرها في مكان عام (مثلًا في القاعات المجتمعية). وذلك بهدف إيجاد الشفافية وإبلاغ المجتمع الذي تم اختياره بناءً على معايير الاستهداف المتفق عليها. كما أنه يعطي فرصة لأولئك الذين ليسوا على القائمة ولكنهم يستوفون متطلبات الاستهداف ليتم تضمينهم في البرنامج. ستحتوي هذه القائمة على بيانات شخصية، لذلك سيكون من المهم تقليل ما يتم مشاركته بشكل عام. عادةً ما يكون الاسم والموقع العام كافيين، والتفاصيل أو البيانات المستخدمة في التحقق من الاستهداف ليست ضرورية. ومع ذلك، فإن معرفة أن قائمة الأسماء مرتبطة ببعض المعايير المحددة (حتى التفاصيل التي تم فيها استيفاء المعايير أم لم يتم) توضّح للجمهور الأوسع أمورًا عن الأفراد المدرجين قد تؤدي إلى مشكلة بالنسبة لخصوصيتهم. إن وجود مشكلة في ذلك من حيث حماية البيانات يعتمد على السياق. في قرية صغيرة حيث تكون الظروف المعيشية لجميع السكان معرفة عامة على أي حال (بمعنى أنهم يمتلكون أو لا يمتلكون الخصائص التي تتوافق مع المعايير المستهدفة)، قد لا يكون نشر القائمة مشكلة من حيث الخصوصية. على العكس من ذلك، في سياق يعيش فيه المستفيدون في سرية نسبية، قد يكون نشر القائمة مشكلة. من المحتمل أن يتعارض نشر المعلومات التي لم تكن معروفة للجمهور مسبقًا مع مبدأ السرية. بالتالي من المستحسن النظر بعناية في السياق قبل اتخاذ قرار بنشر القائمة أو عدم نشرها.

بالإضافة إلى ذلك، وبعد عملية التحقق أو التأكد من الأهلية، يجب التعامل مع بيانات أولئك الذين يعدّون غير مؤهلين بشكل مسؤول (مثلًا، أرشفة البيانات بشكل آمن إذا كانت هناك متطلبات تدقيق، أو إنشاء قائمة مبسطة يتم الاحتفاظ بها لتجنب إعادة التحقق، أو حذفها إذا لم يكن هناك حاجة لها). يمكن العثور على مزيد من التفاصيل حول هذا الأمر في فصل التوجيهات العامة.

أمثلة على الضرورة والتقليل من جمع البيانات أثناء عمليات التحقق من الأهلية:

في سياق البرنامج، فإنّ المعيار المستهدف هو "الأسر التي ترعى أشخاصًا من ذوي الإعاقة". للتحقق من الأهلية، من الضروري معرفة وجود أفراد فعليين ممن يعانون من الإعاقات ويعيشون مع تلك الأسر. قد يكون من المفيد معرفة طبيعة الإعاقة التي يعانون منها. عند التحقق من الحقائق، سيكون من الممكن الكشف عنها خلال الزيارات المنزلية مثلًا. لكن من غير الضروري العودة إلى السجلات الطبية للتحقق من الإعاقة، فالقيام بذلك قد يؤدي لكشف بيانات شخصية حساسة ليست ذات صلة بالبرنامج.

يقترح قادة المجتمع استهداف الأمهات العازبات اللاتي لديهن ثلاثة أطفال على الأقل ولا يملكن دخلًا ماليًا كفئات أكثر ضعفًا، وإيجاد قائمة أولية بناءً على هذا المعيار. يتم التحقق من المعلومات التي يوفرها قادة المجتمع من خلال الزيارات المنزلية حيث يتم تحديد المستفيد وسؤاله عن أعمار جميع أفراد المنزل. للتحقق من الدخل، قد يكون من الضروري السؤال عن مصدر دخل المستفيد. لكن قد لا يكون من الضروري جمع معلومات إضافية مثل عمر الأم وانتمائها الديني لأن ذلك لن يؤثر على قرار استهداف هذا المستفيد. كما أنه من غير الضروري السؤال عن أرباب العمل السابقين أو طلب كشف حساب بنكي لتحديد مستوى الدخل.

في سياق الاستجابة لمجاعة، فإن معيار الاستهداف من أجل برنامج المبالغ النقدية هو «الأسر التي يعيلها أطفال وتعاني عدم وجود أمن الغذائي». قد لا يكون من الضروري السؤال عن تعليم الأطفال عند التحقق من الأهلية. لن يؤثر المستوى التعليمي على التحقق من الأهلية أو المبالغ التي سيتم منحها.

ملاحظة: عند إجراء عمليات جمع البيانات أو معالجتها، من المهم مراعاة أن يتم التعامل مع البيانات الشخصية بشكل آمن. وسواء تم جمع البيانات على الورق أو تطبيقات الهواتف المحمولة أو أي وسائل أخرى، يجب ضمان أن تكون البيانات قابلة للوصول فقط من قبل أولئك الذين يحتاجون إلى الوصول إليها بشدة. يجب مراعاة أمن البيانات في كافة المراحل بما في ذلك حذف أي بيانات لضمان عدم إمكانية استعادتها. يمكن العثور على مزيد من التفاصيل حول هذا الأمر في فصل التوجيهات العامة.

قرار المشروع 3: هل يجب علي التحدث مع المستفيدين بشأن التعامل مع بياناتهم في هذه المرحلة؟

الشفافية

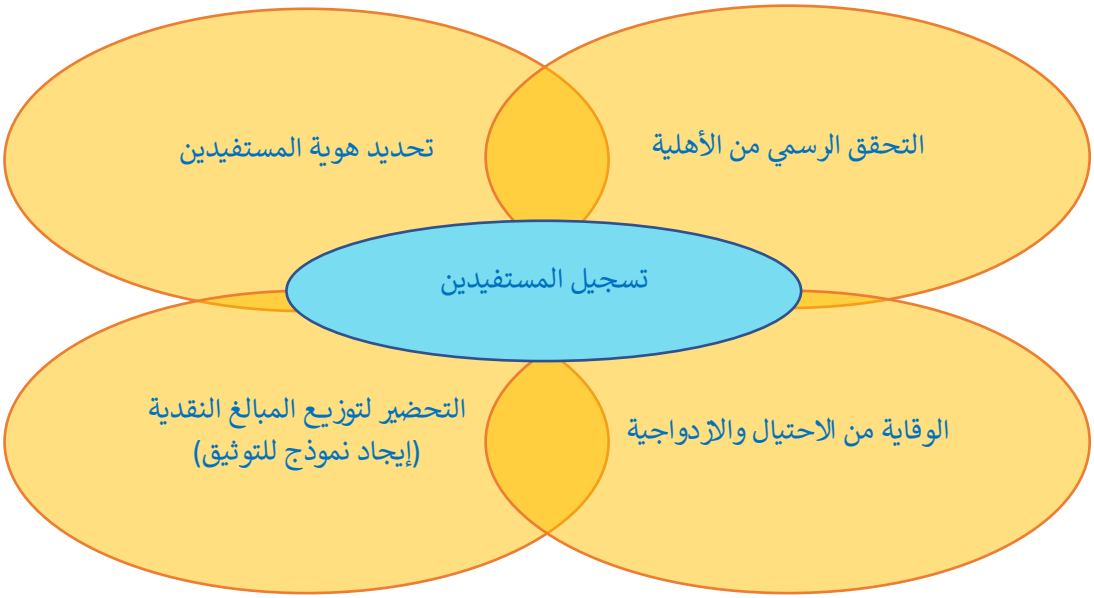
إعادة صياغة مشروع القرار: كيف يمكنني التأكد من أن المستفيدين قادرون على الوصول إلى المعلومات المتعلقة بمعالجة بياناتهم؟

الشفافية مبدأ مهم لحماية البيانات. في سياق التحقق من الأهلية، قد يكون جمع المعلومات أقل رسمية من تسجيل المستفيد. رغم ذلك، من المهم أن يعرف المستفيدون ما الذي يحدث للمعلومات التي يشاركونها معك. يتضمن فصل تسجيل المستفيد معلومات أكثر عن كيفية إعلام المستفيدين، إلا أنه من الجيد مراقبة هذه المعايير عند إجراء التأكد أو التحقق من الأهلية. بعض المعلومات التي ينبغي إعلام المستفيد بها:

- من أين حصلت على المعلومات الأولية عنهم (مثلًا من أعضاء المجتمع، أو القوائم الحكومية، أو المنظمات الأخرى)؟
- سبب إجراء التحقق من الأهلية
- إمكانية تصحيح البيانات غير الدقيقة في أي وقت
- إمكانية مشاركة البيانات التي تم الحصول عليها مع مؤسسات أخرى والهدف من تلك المشاركة (في حال كانت ستتم مشاركتها)

IV. تسجيل المستفيدين

استخدام البيانات الشخصية



شكل 2: أهداف تسجيل المستفيدين

يحدث التسجيل الرسمي للمستفيدين عادة بعد إنشاء قائمة بالمستفيدين المستحقين (انظر القسم 4_4M من مجموعة أدوات توزيع المبالغ النقدية في حالات الطوارئ CiE لمزيد من التفاصيل). هذا يتضمن جمع بيانات شخصية وإدارة تلك البيانات لتوزيع ومراقبة البرنامج. يوضح الشكل 2 الأهداف الأساسية لتسجيل المستفيدين، وتوضح الأمثلة أدناه استخدام البيانات الشخصية:

- **التحديد.** في بداية عملية التسجيل، يُطلب من رب الأسرة عادة إبراز إثباتات شخصية (مثلًا رخصة القيادة أو بطاقة الضرائب أو بطاقة التصويت) للتأكد من أنه الشخص المدرج على قائمة المستفيدين. سيحتوي إثبات الشخصية على الاسم وتاريخ الميلاد والبيانات الشخصية الأخرى المذكورة مسبقًا في التسجيل. قد يُطلَب من

المستفيد التزويد بقياسات حيوية (مثل بصمات الأصابع) لتوثيق أكبر ولضمان أنه لم يتم تسجيلهم عدة مرات. تعد تلك القياسات الحيوية بيانات شخصية ويمكن أن تكون حساسة.

- **التحقق الرسمي من الأهلية.** يُطرح على المستفيد أسئلة تتعلق بمعايير الاستهداف في حال لم يتم إجراء عملية التحقق بشكل رسمي من قبل، وفي حال كان هناك تغير في البيانات منذ وقت الاستهداف--لضمان أن المستفيد لا يزال مستحقًا قبل توزيع المبالغ النقدية.
- **التحضير لتوزيع المبالغ النقدية.** حيثما يمكن فعل ذلك، يُطلب من المستفيد التزويد بمعلومات مثل معرفة العميل أو أي معلومات أخرى يطلبها مزود الخدمة المالية لتوزيع المبالغ النقدية عليهم (مثلًا رقم الهاتف المحمول للمبالغ المحوَّلة أو تفاصيل الحساب المصرفي).
- **إنشاء نموذج للتوثيق.** يُزوَّد المستفيد ببطاقة مستفيد من الصليب الأحمر مع صورة ومعرّف خاص يمكن إبرازه أمام مزود الخدمة المالية كدليل على أهليتهم وتسجيلهم المسبق. وهي مفيدة بشكلٍ خاص عند عدم توفّر بطاقة تعريف رسمية.
- **الوقاية من الاحتيال والازدواجية.** للوقاية من الاحتيال والازدواجية، قد يُطلَب من المستفيدين التزويد ببيانات شخصية تتعلق بأفراد العائلة أو البيانات الحيوية.

اعتبارات حماية البيانات

سيتضمن إجراء تسجيل المستفيدين جمع ومعالجة البيانات الشخصية بناءً على الأهداف الأساسية الموضحة أعلاه. يتناول هذا القسم قرارات المشروع الأساسية في عملية التسجيل واعتبارات تتعلق بحماية البيانات.

قرار المشروع 1: كيف يمكنني التحقق من هوية المستفيد؟

تقليل البيانات، ضرورة

إعادة صياغة مشروع القرار: أي آليات التحقق فعالة وتتدخل بأقل قدرٍ ممكن بمصالح المستفيدين (بما في ذلك السرية)؟

للتحقق من هوية الأفراد الذين أتوا للتسجيل، يُطلَب إبراز معرّف خاص. يمكن أن يكون المعرف الخاص ورقيًا (مثل رخصة القيادة أوبطاقة الهوية الشخصية الوطنية، إلخ.) أو قياسات حيوية (مثل البصمات أو مسح قزحية العين، إلى أخره.). عند اختيار إحدى تلك الخيارات، ينبغي أن تؤخذ بعض الجوانب العملية وحماية البيانات بعين الاعتبار. في بعض السياقات، قد لا يكون من المفيد طلب إبراز الهوية الشخصية عندما لا يتوفر في المجتمع توثيقات كتلك. في سياقات أخرى، قد يبدو جمع البيانات الحيوية الطريقة الأكثر فعالية والوحيدة التي تمنع الاحتيال. من وجهة نظر حماية البيانات، من المهم أن نضع في الاعتبار أن بعض البيانات أكثر حساسية من غيرها. الهدف هو جمع البيانات الأقل حساسية كلما أمكن ذلك.

التعريف الورقي

في العديد من المناطق، تكون الطريقة الأسهل والأكثر شيوعاً هي طلب البطاقات التعريفية، مثل بطاقات الهوية الوطنية أو جوازات السفر الصادرة عن الحكومة. لا يشكل طلب هذه المُعرفات خطورة كبيرة من منظور حماية البيانات، لأن هذه المستندات تخدم بالضبط لغرض تحديد هوية المالك. إن ضرورة إجراء مسح ضوئي أو نسخ وتقديم هوية كل مستفيد هي مسألة منفصلة. لغرض تحديد الهوية، غالبًا ما يكون كافيًا أن تطلب من المستفيد تقديم هويته إليك عند التسجيل وتدوين رقم الهوية المتفرد. يمكنك تحديد المربع الذي يؤكد أنه قد تم التحقق من الهوية دون الاحتفاظ بنسخة كاملة من الهوية. قد يتم قبول بطاقات الهوية أو المستندات البديلة مثل رخصة القيادة وشهادة الميلاد وشهادة التعميد وفواتير الكهرباء بدلاً من بطاقة الهوية الوطنية إذا لم يكن لدى تتوفر من المجتمعات هذه الهوية. وعند جمع هذه الوثائق، يوصى مرة أخرى بجمع أقل قدر ممكن للتحقق من الهوية. وليس الأكثر دائما أفضل في سياق حماية البيانات. وبالإضافة إلى ذلك، يوصى بعدم طلب وثائق تحتوي على بيانات حساسة (*مثل* الأوراق المتعلقة بالصحة). كما أنه قد لا يكون من الضروري، كما نوقش، الاحتفاظ بنسخ من هذه الوثائق.

البيانات الحيوية

البيانات الحيوية هي بيانات تتعلق بالخصائص الفسيولوجية أو السلوكية للشخص المعترف بها بالوسائل التكنولوجية. ومن الأمثلة النموذجية على ذلك بصمات الأصابع الرقمية، ومسح القزحية، ومسح كف اليد، والتعرف على الوجه والصوت. وتعتبر هذه البيانات حساسة للغاية كما هي شخصية للغاية وليس شيئا يمكن استبداله فقط إذا تعرضت للخطر، وبالتالي تستحق مستوى أعلى من الحماية. في بعض الحالات، تخضع البيانات الحيوية لقيود قانونية بما في ذلك تقييد الاستخدام أو حظره. والسبب الرئيسي لذلك هو احتمال إساءة استخدام هذه البيانات:

- **إنفاذ القانون أو الأمن.** يمكن أن تكون البيانات الحيوية مثيرة للاهتمام للغاية للجهات الفاعلة في إنفاذ القانون أو الأمن ، لأنه لا يمكن تعديلها. عند جمع مثل هذه البيانات في سياق مشروع ما، قد تتعرض لضغوط من أطراف أخرى للكشف عن تلك البيانات لأغراض أخرى.
- **سرقة الهوية.** البيانات الحيوية هي أيضا أكثر عرضة للاختراق لسرقة الهوية لأنها فريدة من نوعها بحيث لا يمكن تعديلها.
- **مصدر المعلومات في المستقبل.** من الممكن أن تستخدم البيانات الحيوية التي يتم جمعها اليوم في المستقبل لمعرفة المزيد عن الفرد أكثر مما هو ممكن حاليا. وقد تكون الحلول التكنولوجية الجديدة قادرة على قراءة معلومات أخرى، مثل التفاصيل الوراثية.

وبالتالي، فإن جمع البيانات الحيوية[2] يشكل خطرا كبيرا وينبغي اعتباره الملاذ الأخير. ويجب تقييم جمع هذه البيانات لتحديد ما إذا كان ذلك ضروريا للغاية أو ما إذا كان يمكن استخدام حل بديل. وينبغي النظر في سياق المشروع وكذلك مسؤولية المنظمة وقدرتها على حماية تلك البيانات بعناية. وحتى عندما يبدو أن البيانات الحيوية هي أفضل طريقة للتحقق من هوية الأفراد وتجنب الاحتيال، فلا يزال يتعين تقييم المخاطر المحتملة للمستفيدين. وعلى وجه الخصوص، إذا كان من المرجح أن الجهات المعنية الأخرى يمكن أن يطالبوا بتلك البيانات لأغراضهم الخاصة، فإن هذا الخطر قد يفوق المزايا العملية للبيانات الحيوية. وبالإضافة إلى ذلك، عند جمع البيانات الحيوية، فإن الاعتبارات المتعلقة بالتخزين الآمن المأمون أكثر أهمية (انظر الفصل التوجيهي العام).

وعلاوة على ذلك، تذكر الحق في تلقي المعلومات (الشفافية). ويجب تقديم هذه المعلومات بطريقة يمكن للأفراد فهمها. وقد لا يكون الإلمام العام بالقراءة والكتابة و/أو الوعي بالقياسات الحيوية كافيا لتمكين الناس من فهم المخاطر المرتبطة بهذه العملية (تجدر الإشارة إلى أنه ينبغي دائما النظر في بدائل التسجيل الحيوية، انظر مقرر المشروع 3 أدناه).

مثال:

وقد تأثرت عدة مناطق جغرافية بجائحة أدت إلى فقدان سبل العيش. تم الاستقرار على إجراء تدخل نقدي لمجتمع حضري متطور ومجتمع آخر في مجتمع ريفي بعيد. للتسجيل، طلب من أرباب الأسر المتضررة في السياق الحضري أن يجلبوا شكلا واحدا من أشكال الهوية من قائمة بالاستمارات والوثائق السارية لإثبات هويتهم. بالنسبة للمجتمع الريفي، طلب من أرباب الأسر أن يجلب شهادة من زعماء/رؤساء قُراهم لأنهم يفتقرون إلى الشهادات الرسمية. ثم قدمت الجمعية الوطنية للمستفيدين من المنطقة الريفية بطاقة هوية مؤقتة لتقديمها إلى مقدم الخدمات المالية عند المطالبة بالنقد المستحق لهم. في كلتا الحالتين، تم تجنب جمع بيانات القياسات الحيوية لتحديد الهوية، واستُخدمت وسائل أخرى لكشف الغش والازدواجية مثل التحقق من أسماء وأعمار أفراد الأسرة وإصدار قسيمة استخدام لمرة واحدة مع كود شريطي فريد تم مسحه ضوئيا بعد تلقيهم أموالهم للإشارة إلى أنهم قد حصلوا بالفعل على مستحقاتهم.

قرار المشروع 2: ما هي البيانات الأخرى التي يجب أن أجمعها من المستفيدين أثناء التسجيل؟

تقليل البيانات، ضرورة

إعادة صياغة مشروع القرار: ما هي بيانات المستفيدين الأخرى الضرورية للبرنامج؟

وإلى جانب جمع البيانات لتحديد الهوية، هناك أنواع أخرى من البيانات التي تم جمعها أثناء التسجيل لأغراض أخرى مذكورة أعلاه. ولهذه الأغراض، من المهم أن تُفكر أي من تلك البيانات تُعتبر ضرورية للغاية. حاول أن تسأل نفسك: ما هو الشيء الذي سأحتاج لاستخدام هذه البيانات فيه وهل هي ضرورية لبرنامجي؟ إذا كنت غير متأكد أو إذا كنت تعتقد أنه يمكنك تحقيق الغرض باستخدام بيانات أخرى أو بطرق أخرى ، فخذ بعين الاعتبار عدم جمع تلك البيانات. في بعض الأحيان هناك ميل إلى جمع أكثر من اللازم لأننا نعتقد أن البيانات قد تصبح مفيدة في وقت لاحق أو لأننا دائما نجمع تلك المعلومات، أو أننا بحاجة إليها لقاعدة البيانات لدينا. إنشاء

[2] لمزيد من المعلومات، يرجى الاطلاع على الفصل الخاص بحماية البيانات حول القياسات الحيوية. بالإضافة إلى سياسة القياسات الحيوية للجنة الدولية للصليب الأحمر.

قاعدة بيانات ليس سببا مؤهلا لجمع المعلومات. بل على العكس من ذلك، يجب أن يكون كل عنصر من عناصر البيانات الشخصية في قاعدة البيانات تلك موجودا لسبب محدد، من أجل شيء واضح المعالم وهام جداً للبرنامج.

استخدام نماذج موحدة

للتسجيل، استخدام نماذج موحدة شائع ومفيد جداً لأنه يسرع جمع البيانات لأنه تم تحديد أنواع البيانات المستخدمة عادة. ومع ذلك، يميل أستخدام هذه النماذج إلى تغطية مجموعة واسعة من البيانات بهدف جعلها استبياناً مناسب للكل. ولكن في حالات الطوارئ، يمكن استخدام هذه النماذج كما هي في مقابل كونها ذات طبيعة تحليلية للبيانات ذات الصلة والأساسية في البرنامج الحالي الجاري تنفيذه. جمع الإجابات على تلك الأسئلة غير ذات الصلة يتعارض مع مبدأ تقليل جمع البيانات إلى أدنى حد وعند الضرورة. هذا لا يعني أنه يجب عدم استخدام هذه النماذج. ولكن بدلا من ذلك، خذ بعض الوقت لتحليل وتكييف النماذج لكل تدخل. التكيف لا يعني إعادة إنشاء نماذج جديدة في كل مرة، ولكن بدلا من ذلك يمكنك استخدام نفس النموذج ولكن تخطي الأسئلة التي ليست لها حاجة (أي، لا تسأل إذا كان طرح الأسئلة لفظيا). في ملفات Excel يمكن إخفاء أعمدة أو صفوف معينة؛ في النماذج الورقية يمكن تنقيح بعض المقاطع أو شطبها ، وفي حقول النسخة الرقمية يمكن وضع علامة أنها غير مطلوبة [3] أو مخفية. سيحتاج أعضاء الفريق الذين يقومون بجمع البيانات إلى إبلاغهم بمبدأ تقليل البيانات إلى أدنى حد، حتى يفهموا سبب تخطي بعض الأسئلة عمدا.

أمثلة:

في برنامج نقدي يستهدف "الأسر المعيشية التي فقدت سبل عيشها". وفي يوم التسجيل ، يطلب من المستفيدين ملء النموذج الموحد الذي تصدره الجمعية الوطنية. وقد قام الفريق بتحليل النموذج مسبقا وقرر أنه ينبغي للأسر أن تجيب على جميع الأسئلة المتعلقة بالنموذج المتعلق بوضعها الاقتصادي. ومع ذلك ، قام الفريق بشطب جميع الأسئلة المتعلقة بالحالة الصحية لأفراد الأسرة. ولا يجوز تقديم هذه المعلومات، لأن الأسر المعيشية ستحصل على نفس المساعدة النقدية، سواء أكانوا مرضى أم لا.

وتستجيب الجمعية الوطنية لحالة الطوارئ الناجمة عن الجفاف. ولديهم أيضا برنامج ضخم للتبرع بالدم. ويستخدم الفريق نموذجاً معيارياً يتضمن أسئلة تتعلق بنوع الدم لدى المستفيدين. وبما أنّ هذه المعلومات ليست ذات صلة مباشرة بالاستجابة لحالات الطوارئ المتعلقة بالجفاف التي يعملون عليها ، فقد قرروا عدم طلب هذه المعلومات من المستفيدين والمتطوعين الذين يقومون بجمع البيانات وقد تمّ إبلاغهم بالسبب. ويمكن، كبديل عن ذلك ، توضيح أنّ المستفيدين يمكن أن يقدموا بصورة اختيارية معلومات عن أنواع الدم إذا رغبوا في المشاركة في جهود التبرع بالدم ، ولكن هذه المشاركة لن تؤثر على أي صرف للتعويضات.

وفيما يلي أهداف مختلفة لجمع البيانات والاعتبارات الرئيسية لحماية البيانات:

التحقق رسميا من الأهلية

وعلى الرغم من أن المستفيدين المؤهلين هم وحدهم المدعوون للتسجيل ، فإن التحقق الذي تم أثناء عملية تحديد الأهداف لم يكن رسميا بما فيه الكفاية أو أن الوضع قد تغير مما يجعل من الضروري إعادة التحقق من الأهلية أثناء عملية التسجيل. وهنا ، سيتعين جمع البيانات المتعلقة بمعايير الاستهداف المتفق عليها. وقد سبق أن نوقشت الاعتبارات المتعلقة بذلك في فصل الاستهداف. وتنطبق تلك الاعتبارات أثناء عملية التسجيل ، ولا سيما مسألة ما إذا كانت بعض المعلومات ستؤثر على قرار استهداف شخص ما. وإذا كان الأمر كذلك ، يمكن جمع هذه المعلومات. وإلا فليس هناك ما يدعو إلى ذلك.

[3] لاحظ وجود تمييز هنا بين البيانات التي تم وضع علامة عليها على أنها "غير مطلوبة" حتى لا يكون من الضروري طرحها في حالة الحاجة إلى الإجابة على هذا السؤال للاستمرار في استبيان رقمي ، مقابل "اختياري" حيث لا يزال السؤال يطرح ويكون الأمر متروكا للمستجيب سواء كان يجب إعطاء إجابة أم لا. تحتاج بعض الأسئلة الاختيارية إلى إعادة النظر من قبل نظام حماية البيانات. أولاً، لا ينبغي جمع المعلومات الغير ضرورية. وحتى عندما يتم جمع البيانات بشكل تطوعي، ينبغي تطبيق مبدأ تقليل البيانات. ثانياً ما زالت تدعو الأسئلة الاختيارية الناس إلى إعطاء هذه المعلومات وربما تخلق انطباع أنهم يحظون بفرص أفضل للحصول على المساعدة إذا اخبرونا المزيد من المعلومات، وأخيراً إن المعلومات التي تُعطى وحتي أن لم تُطلب بشكل مباشر للمشروع فسيتوجب علينا اعتبار أنه يوجد أساس قانوني لتجهيز هذه البيانات. ويجدر بالذكر والتي ينبغي شرحها بوضوح للمستفيدين أنه عند طلب المعلومات «الاختيارية» أن تقديم هذه المعلومات لا يؤثر بأي شكل على المساعدة.

وفي التوزيع الشامل حيث لا توجد معايير محددة للأهداف لأن المتضررين في منطقة ما يحتاجون جميعا إلى المساعدة ، قد لا يكون جمع بيانات الأهلية ضروريا ما لم تكن هناك حاجة إلى التأكد من أنهم من المنطقة المتضررة أو إثبات التوثيق لجمع المساعدة. ولا تتطلب عملية التسجيل في هذه الحالة سؤالا عن مؤشرات الضعف أو غيرها من المسائل المستخدمة عادة لإثبات الأهلية. كما أن طرح الأسئلة لجمع البيانات الديموغرافية النموذجية (مثل العمر ، والجنس ، وحجم الأسرة) قد لا يكون ضرورياً أيضاً ، إلا إذا كان لها غرض ذي صلة نظراً لعدم استخدام مثل هذه البيانات لاستهداف المستفيدين.

توزيع نقدي منفذ

وتتوقف البيانات المطلوبة لتمكين المستفيدين من التوزيع النقدي على طريقة التوزيع المختارة. وفيما يتعلق بالنقد الموجود في المغلفات ، قد تقتصر البيانات الرئيسية المراد جمعها على معلومات الهوية والتوثيق الأساسية التي تستخدم أثناء التوزيع. عند استخدام مقدمي الخدمات المالية ، قد تكون هناك حاجة إلى المزيد من البيانات بما في ذلك بيانات معرفة زبونك المطلوبة بموجب القانون من أجل توزيع الأموال. وستناقش تفاصيل جمع البيانات التي تستخدمها شعبة الخدمات المالية بمزيد من التفصيل في الفصل التالي. أثناء عملية التسجيل ، من الأهمية بمكان أن نراقب ما هو مطلوب وضروري للسماح بالتوزيع النقدي (على سبيل المثال ، الأرقام المتنقلة لاستقبال الأموال المتنقلة).

منع الاحتيال والازدواجية

ولتجنب الغش وازدواجية المدفوعات ، قد يكون من الضروري جمع معلومات إضافية لتحديد المعلومات الأساسية للأسر المعيشية. فعلى سبيل المثال ، جمع أسماء جميع أفراد الأسرة وأعمارهم ونوع جنسهم وإجراء فحص إذا حاول أي منهم التسجيل كأسرة معيشية منفصلة. كما أن البرامج التي تعتمد على حجم الأسرة لتحديد حجم النقد المطلوب صرفه قد تكون مطلوبة للتحقق التفصيلي من الأسر (على سبيل المثال ، باستخدام بطاقات الأسرة التي تصدرها الحكومة). وفي هذه الحالات ، من المهم التفكير في السياق الفعلي لتقييم المخاطر ، ثم ضمان أن يكون جمع البيانات وتجهيزها ملائمين لمستوى المخاطر المقدرة ، بدلا من جمع هذه البيانات بطريقة موحدة.

أمثلة:

وقد وضع برنامج نقدي استجابة للحرارة الشديدة التي تسبب الحرائق في قرية صغيرة. إن المعيار المستهدف (الأسر التي فقدت منازلها) يشمل تقريباً كل أسرة في القرية. ويشير زعماء المجتمع المحلي إلى أسماء رؤساء تلك الأسر المعيشية ويؤكدونها. وفي يوم التسجيل ، يُطلب من رؤساء الأسر المعيشية تحديد هويتهم. ويقرر الفريق عدم جمع البيانات المتعلقة بأفراد الأسرة. وخطر الغش ليس مرتفعا جدا ، لأن معظم الأسر المعيشية ستتلقى المساعدة ، وقد تم تحديد أرباب هذه الأسر بوضوح وإدراجهم في القائمة بالتعاون مع المجتمع المحلي. وبالتالي، من غير المرجح أن يتمكن أفراد الأسرة الآخرون أو الأشخاص القادمون من قرى أخرى من طلب المساعدة زورًا.

وقد وضع برنامج نقدي لمواجهة انعدام الأمن الغذائي في مجتمع محلي صغير يستهدف الأسر المعيشية التي ترأسها نساء. وتتناسب المنحة النقدية مع حجم الأسرة المعيشية لتلبية احتياجاتها. ويقرر فريق البرنامج جمع حجم الأسرة المعيشية لأنه ضروري لحساب المنح ، ولكن من غير الضروري على الأرجح جمع معلومات إضافية عن أفراد الأسرة. وبما أن المجتمع المحلي صغير ، فمن غير المرجح أن يحاول الناس الإشارة إلى أرقام أعلى عن حجم أسرهم المعيشية لأن من المرجح أن يعرف أفراد المجتمع الآخرون هذا التباين ويبلغوا عنه.

وقد بدأ تنفيذ نفس البرنامج النقدي في مجتمعات أوسع نطاقا وأكثر تشتتا. والمنح النقدية أعلى بسبب تسويات تكلفة المعيشة. ووردت بعض التقارير عن ارتفاع أحجام الأسر المعيشية في البرامج السابقة التي تديرها منظمات غير حكومية أخرى. وأشار تحليل فريق البرنامج إلى ارتفاع مخاطر الاحتيال المحتمل وقرر جمع البيانات الإضافية حول أفراد الأسرة (الاسم والعمر والجنس ودرجة القرابة أو العلاقة بالأسرة). واستخدمت بيانات إضافية للتدقيق المزدوج في قائمة المستفيدين المسجلين.

ملاحظة: وفيما يتعلق بالبرامج التي تستخدم الاستهداف الذاتي أو التسجيل الذاتي ، حيث ينطبق المستفيدون على أساس معايير الهدف المنشورة، من المهم ملاحظة أن البيانات تُجمع أيضا لمن لا يستوفون الأهلية. يوصى بالتأكد من حذف أو أرشفة البيانات للأفراد الذين من الواضح انهم غير مؤهلون وذلك لمنع محاولات إعادة التسجيل (حسب الضرورة). إذا اقتضت الحاجة المزيد من البيانات لتأكيد هوية الفرد، تخزن البيانات لوقت محدود حتى تنتهي عملية تأكيد الهوية وأن كان الفرد غير مؤهل نخبره بذلك وبعدها نمسح بياناته. أنظر إلى فصل الاعتبارات العامة لتسجيل بيانات الغير مستفيدين. وأيضاً تأكد من أن تكون المعايير المستهدفة المنشورة محددة ومفصلة للحد من أعداد المتقدمين الغير مؤهلين.

قرار المشروع 3: ماذا يجب أن اخبر المستفيدين عن كيفية إدارتهم لبياناتهم؟

الشفافية

إعادة صياغة مشروع القرار: كيف يمكنني التأكد من أن المستفيدين قادرون على الوصول إلى المعلومات المتعلقة بمعالجة بياناتهم؟

يوضح مبدأ الشفافية لحماية البيانات بأن على المستفيدين وبصفتهم موضعين بيانات أن يتلقوا معلومات واضحة حول أسباب جمع بياناتهم وكيفية إدارتنا لبياناتهم. هذا يشمل الغرض من جمع وتخزين وربما نشر بياناتهم وحقوق المستفيدين والى آخره... ربما سيشكل أعلام المستفيد تحدياً صعباً في بعض الحالات وخصوصاً في حالات الطوارئ حينما يكون الوقت محدود. وبالإضافة إلى ذلك، فأنه حينما يملك المستفيدين احتياجات طارئة وملحة اكثر من حماية بياناتهم فأنهم قد لا يظهرون الاهتمام بسماع التفاصيل أو فهم ماذا تعني حماية بياناتهم. وبالرغم من هذا، فهم لديهم الحق بسماع هذه المعلومات.

أن افضل حل هو بإعطاء المستفيدين بعض **المعلومات الأساسية ومعلومات للتواصل** في حالة رغبتهم بمعرفة المزيد. يجب تضمين هذا في خطة المشاركة المجتمعية والاعتمادية للبرنامج (انظر في الوحدة 2_4M من أدوات النقد في حالات الطوارئ). يمكن توفير المعلومات الأساسية أثناء المقابلة مع المجتمعات لتوضيح البرنامج ويمكن تكرارها أثناء عملية تسجيل المستفيدين. وأيضاً يمكن توفير إشعار عام بشأن سياسة الخصوصية مع بعض التفاصيل عن البرنامج لتطبعها وتنشرها الجمعية الوطنية (أنظر إلى نموذج إشعار الخصوصية في قسم المراجع). وللمزيد من المعلومات باستطاعة المستفيدين مناقشة هذا الإشعار والتواصل مع الجمعية الوطنية عند الحاجة. أن الهدف هو أمكانية المستفيدون التواصل معنا إما عن طريق الخط الساخن لمن لديهم إمكانية الوصول إلى الهاتف أو بالتواصل شخصياً معنا.

عند تزويد المعلومات حول معالجة البيانات، من المفضل أن تضع نفسك مكان المستفيدين وتسأل ذاتك هذا السؤال: ماهي المعلومات التي احتاج إلى معرفتها قبل إعطاء بياناتي الشخصية؟ المعلومات الأساسية العامة مدرجة أدناه. يجب تقديم هذه المعلومات بكل وضوح في أسلوب سلس وواضح وبالكلمات المفهومة والملائمة.

- **الهدف من جمع البيانات في يوم التسجيل.** ارجع إلى الأهداف التي حددها برنامجك، شرحنا بعض الأهداف الشائعة في أعلاه التي تتضمن الحاجة إلى إثبات الهوية والتحقق من الأهلية وتفعيل التوزيع النقدي أو تجنب الاحتيال والازدواجية. على المستفيدين معرفة هذه الأسباب وسبب الحاجة إلى بيانات معينة لهذه الأهداف، يساعدهم هذا في فهم ماذا يحصل لبياناتهم.
- **إذا جمعت بياناتهم من الآخرين** (على سبيل المثال: من منظمات غير حكومية أخرى أو من قادة المجتمع أو من الحكومة). غالباً ما تتلقى معلومات عن المستفيدين من مصادر أخرى قبل أن تتواصل معهم مباشرةً. من الهام أن يعرف المستفيدون من أين حصلت على معلوماتهم الخاصة لكي يشعروا بالثقة في أن بياناتهم يتم استخدامها بشكل مسؤول.
- **كيفية تصحيح البيانات الخاطئة.** بالنسبة للمستفيدين، من المريح معرفة قدرتهم على تصحيح المعلومات الخاطئة في أي وقت. تحصل الأخطاء بالأخص حين تحدث الإجراءات على عجل أثناء حالة الطوارئ، حيث تحصل الأخطاء من كلا الطرفين من فريق البرنامج الذي يجمع البيانات أو من المستفيد الذي يقدم البيانات الأولية. إذا وجد المستفيد إن بعض المعلومات خاطئة يجب أن تكون له الصلاحية في طلب تصحيح.
- **كيفية التعبير عن المخاوف أو تقديم شكوى.** يجب أن يعي المستفيدون حقهم في التعبير عن مخاوفهم حول التعامل مع بياناتهم. من المهم بالنسبة لهم معرفة ذلك لأنه يمنحهم إحساساً بالسيطرة. قد يرغب المستفيدون الاعتراض على معالجة البيانات أو تقديم شكوى بشأنها. في هذه الحالة، يجب أن تكون لديهم معرفة بشأن أين ومع من يجب أن يتحدثوا بخصوص مخاوفهم وخياراتهم المتاحة. يجب أن يكون هذا جزءاً من آلية المراجعة والشكوى للبرنامج (انظر في الوحدة 5_2_4M من أدوات النقد في حالات الطوارئ).
- **النية بمشاركة البيانات.** إذا علمت بأنك سوف تشارك ما تم جمعه من البيانات مع مجموعات أو مؤسسات أخرى (على سبيل المثال:منظمات غير حكومية أخرى، مقدمي الخدمة المالية، الحكومة) يجب على المستفيد معرفة هذا ومعرفة سبب الحاجة إلى مشاركة بياناتهم. بعد كل شيء، فقد وثق بك المستفيد بإعطاء معلوماته فقط لك وأمنك على بياناته. في بعض الحالات لن يغرب المستفيد في أن تشارك بيانات معينة مع كيانات أخرى لأسباب حساسة أو لمخاوف تتعلق بالأمان. قد يكون مفيداً القيام بالعناية الواجبة في مثل هذه المؤسسات حتى تتمكن من إيصال موثوقتيها بشأن تعاملهم مع بيانات المستفيد.

علاوة على ذلك، إذا اكتشف المستفيدون عن سوء استخدام محتمل لمعلوماتهم بسبب مشاركتها مع كيانات خارجية، يجب تشجيعهم على إبلاغ الجمعية الوطنية عن طريق مكتب المساعدة أو الاتصال المباشر بالمختصين بهذه الشؤون.

وبالإضافة إلى المعلومات الأساسية المذكورة أعلاه، سيكون مفيداً تضمين بعض التفاصيل الأخرى حول معالجة البيانات جهزناها في حالة ظهور أسئلة أخرى من المستفيدين. المعلومات الأخرى التي يجب أن يتلقاها المستفيدون (حسب السياق) تشمل:

- كيفية تخزين بياناتهم والتدابير الأمنية
- فترة الاحتفاظ الاحتياطي للبيانات
- الأساسيات المشروعة التي تقام عليها المعالجة
- أي معلومات إضافية أخرى حول الهدف أو مزيد من الإجراءات
- أي معلومات إضافية أخرى حول مشاركة البيانات
- حقوق موضع البيانات التي قد تنطبق، مثل حق المحو وحق الاعتراض وحق الوصول إلى بياناتهم

قرار المشروع 4: هل أطلب الموافقة من المستفيدين؟

الأساس الشرعي

إعادة صياغة مشروع القرار: ما هو الأساس الشرعي الذي يجب أن أعتمد عليه؟

السؤال عما إذا كان يجب أن تطلب من المستفيد الموافقة على جمع واستخدام بياناته له عدة نواحي. لقد أصبح من الممارسات الشائعة بدء استمارات تسجيل المستفيدين بسؤال عن الموافقة قبل المتابعة. للوهلة الأولى، نرى أن الأمر صائب حيث يبدو طلب الأذن أمر مهذب ومحترم. ومع ذلك، بموجب قانون حماية البيانات، يمكن أن تستند معالجة البيانات الشخصية إلى أسباب أخرى غير الموافقة فقط، والتي ستتم مناقشتها بمزيد من التفصيل أدناه.

لكن أليس من الأفضل طلب الموافقة؟ ليس بالضرورة. قد يبدو طلب الموافقة من المستفيد علامة على الاحترام، لكنه يأتي مع بعض التحديات التي يجب مراعاتها.

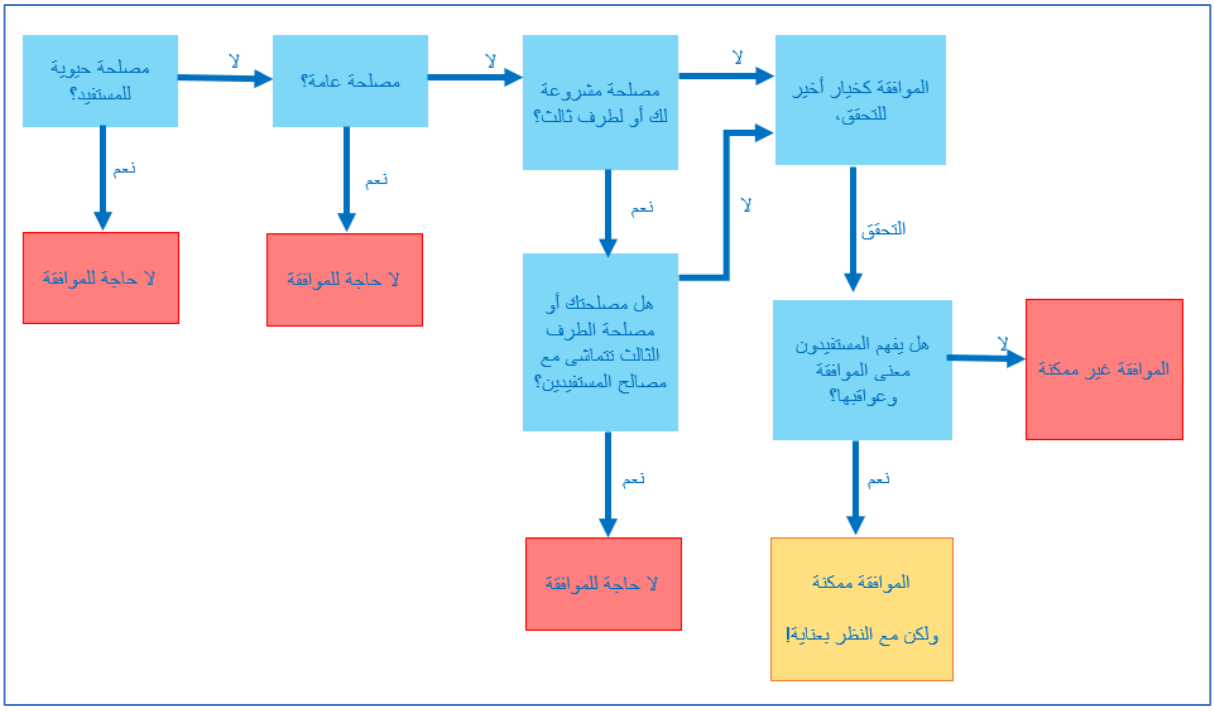
مشاكل في الموافقة

يجب أعطاء الموافقة بحرية دون ضغوط مع علم تام بها. في الممارسة العملية، هذا يعني أن الموافقة تكون صالحة فقط في حالة توفر خيار آخر للمستفيد، غير ذلك فهي لن تكون معطاة بحرية تامة. قد لا يكون طلب الموافقة مناسب في حالات الطوارئ. يحتاج المستفيدون إلى المساعدة الفورية لكونهم ضعيفين ويائسين. قد لا تكون حماية بياناتهم هي أولى اهتماماتهم. ولذلك قد يعطون "الموافقة"[4] لأنهم لا يرون خيار آخر للحصول على الدعم. وبالطبع، من دون بياناتهم لن تستطيع مساعدتهم.

وأيضاً قد يكون المستفيد في وضع لا يسمح له في إدراك عواقب تقديمه لبياناته أو بالكيفية التي تعالج بها بياناته (عن طريق التكنولوجيا مثلاً). لا يمكنك بالفعل الموافقة على شيء لا تستطيع فهمه تماماً (لذا لا نستطيع اعتبار المستفيد على "علم تام" لما يجري لبياناته).

هناك أشكال آخر يجب علينا إيضاحه وهو أن المستفيد قادر على سحب موافقته في أي وقت يشاء (أن أعطي الموافقة بحرية فيستطيع استرجاعها بحرية). لا يسمح بأجراء أي عمليات أضافية في بيانات المستفيد (التي جرت حسب موافقته) حالما يسحب الموافقة. من المحتمل أن يشكل هذا بعض المشاكل للبرنامج لأنه من المهم أن يكون هناك بعض البيانات التي يستطيع البرنامج الاعتماد عليها. حالما يسحب المستفيد موافقته فأنه من المحتمل عدم استطاعتنا العودة واستخدام أساس شرعي مثل المصلحة الحيوية أو المصلحة العامة. لماذا؟ لان حقهم في الانسحاب لن يكون ذو قيمة أن لم يتغير شيء بعد انسحابهم ويعتمد هذا أيضاً فيما إذا كان من الممكن تحديد أساس شرعي آخر وماهي المعلومات التي أعطيت بالفعل إلى المستفيد. ولكل هذه الأسباب فمن الممكن أن تسبب الموافقة بعض الإشكاليات لاستخدامها كأساس شرعي. نوصي بالنظر في خيارات أخرى لمعالجة البيانات الشخصية حسب البرامج النقدية في حالات الطوارئ.

[4] نضع الموافقة بين قوسين لأنه في حين أن المستفيد قد يحدد مربعاً أو قد يشير إلى بعض الإشارات في استمارة التسجيل التي تدل على موافقته، لكن بموجب القوانين والمبادئ العامة لحماية البيانات فأنه ليس من الصحيح الاعتراف به قانونياً.



الشكل 3: مخطط القرار لتحديد فيما إذا كانت الموافقة صالحة كأساس شرعي مقبول

الخيارات الأخرى

يبين الشكل(3) الخيارات الأخرى المتاحة لبناء أساس شرعي. اثنان من هذه الخيارات هما المصلحة الحيوية والمصلحة العامة. **المصلحة الحيوية:** تعني أن معالجة البيانات الشخصية للمستفيدين هي ضرورية لسلامتهم أو صحتهم أو كرامتهم أو امنهم. صممت برامج المساعدات النقدية والقسائم لتلبية الاحتياجات الضرورية في إنقاذ الحياة في بداية حالة الطوارئ وقد تكون مؤهل لتلقي هذه المساعدات ؛ أما في سياق الحالات الغير طارئة في فعاليات المساعدات النقدية والقسائم تحتاج إلى النظر في خيارات أخرى. **المصلحة العامة:** تعني أن معالجة البيانات الشخصية للمستفيدين ستخدم غرضاً في مصلحة الجميع. تقدم الجمعيات الوطنية التي توفر المساعدة مهمة إنسانية تصب بمصلحة الجميع. ولذلك، حتى في حالة عدم الوفاء بالمعايير العالية للمصلحة الحيوية، فأن تلقي المساعدة من برنامج المساعدات النقدية والقسائم سيظل عادة في المصلحة العامة[5].

لتجنب سوء الفهم: يبقى الاختيار بيد المستفيدين فيما إذا أرادوا المشاركة في البرنامج أو لا. لكن إذا قرروا المشاركة، فمن المقبول استخدام بياناتهم الشخصية بدون طلب صريح بالموافقة على استخدامها، بشرط إبلاغهم حول البرنامج وبآلية معالجة بياناتهم. أن هذا في مصلحتهم الحيوية أو/ و في مصلحتهم العامة. المهم هو أن تستخدم البيانات الشخصية الضرورية جداً فقط للبرنامج. راجع أيضاً قسم برمجة التحويلات النقدية في كتيب حماية البيانات للمزيد من التفاصيل حول الأسس القانونية في برنامج المساعدات النقدية والقسائم.

مشاركة البيانات

يمكن لمشاركة البيانات مع كيانات أخرى (مثل: مؤسسات غير حكومية أخرى والحكومة ومقدمي الخدمة المالية) يصب في المصلحة الحيوية للمستفيدين أو في المصلحة العامة. بالإضافة إلى ذلك، يحتمل أن تكون هناك التزامات قانونية لمشاركة بيانات شخصية معينة[6]وإن كان الأمر كذلك فيمكن مشاركتها دون الحصول على الموافقة. أما حينما لا تكون هناك التزامات قانونية فيمكن أن تكون مشاركة البيانات الشخصية في المصلحة المشروعة لمجتمعك الوطني. يمكن أن تبرر مصلحتك المشروعة مشاركة البيانات دون الموافقة في حالة لم يكن للمستفيدين مصلحة غالبة أو متعارضة. من المهم النظر في العواقب أو المخاطر المحتملة للمستفيدين في حالة مشاركة بياناتهم. هذا الموضوع موضح بشكل أوسع في فصل مشاركة البيانات. وباختصار، كل ذلك يعتمد على الضرورة والسرية.

[5] يرجى الملاحظة بأن في بعض الولايات القضائية التي تعتمد على المصلحة العامة من المحتمل أن تطلب اعتبارات إضافية أو موافقة حكومية رسمية. يعد التحقق من ذلك لكل ولاية قضائية خارج أطار هذه الإرشادات. إذا كانت لديك بعض الشكوك فيما إذا كان بمقدارك الاعتماد على المصلحة العامة في برنامجك فرجاءً لا تتردد بالتواصل مع مديرك أو مع الفريق القانوني لجمعيتك الوطنية.

[6] يرجى الملاحظة، أن الامتثال لالتزام القانوني هو أساس شرعي معترف به بشكل عام بموجب قوانين حماية البيانات.

إدارة البرنامج

من المحتمل أن لا تكون بعض قرارات المشروع المتعلقة بمعالجة البيانات في المصلحة الحيوية أو المصلحة العامة مباشرةً لكنها لا تزال معقولة في نظر البرنامج (على سبيل المثال: نوع التخزين وأدراج المزيد من أعضاء الفريق وما إلى ذلك). وهنا مرة أخرى، تأتي المصلحة المشروعة لجمعيتك الوطنية لهيكلة وتنظيم البرنامج في طرق فعالة ومضمونة.

ماذا يعني ذلك؟

ليس من الضرورة الحصول على الموافقة في معظم الحالات. وهذا لا يعني إن أفعالك لن تحاكم، بل على العكس تماماً. مع ذلك، هناك نقطتان أخريان يجب مراعاتهما:

- لا يعني عدم طلب الموافقة بأنك لست بحاجة إلى **إخبار المستفيدين!** ينطبق مبدأ الشفافية، بغض النظر عن الأساس الشرعي الذي تريد استخدامه. كما هو مذكور في قرار المشروع 3: تعتبر بعض المعلومات الأساسية فيما يتعلق بإدارة البيانات الشخصية ومعلومات الاتصال للاستفسار معايير جيدة.
- يمكنك التفكير في تغيير صيغة سؤال الموافقة إلى "هل لديك أي أسئلة أو مخاوف قبل أن نكمل الإجراءات ؟" أو "هل تقر بتلقيك المعلومات الأساسية حول البرنامج بما يتضمن كيفية الحصول على معلومات إضافية فيما يتعلق بطريقة إدارة بياناتك ؟" هذا ليس إلزامياً ولكنه طريقة بديلة لإظهار الأدب والاحترام قبل طلب المزيد من التفاصيل الشخصية.
- هل يتعين عليك تقييم الأساس الشرعي لكل تدخل من تدخلات برنامج المساعدات النقدية والقسائم؟ ليس بالضرورة. من المحتمل أن تغطي معظم تدخلات برنامج المساعدات النقدية والقسائم نفس الأساس الشرعي ، فقط تذكر عدم استخدام الموافقة على أنها الخيار الافتراضي. إذا كانت طبيعة برنامج المساعدات النقدية والقسائم جديدة وفريدة من نوعها ولم تكن التأثيرات على بيانات المستفيد واضحة ، فسيكون من الجيد تقييم الأساس الشرعي رسمياً قبل المتابعة. وفي هذه الحالة، ينصح أيضاً في إجراء تقييم عن تأثير حماية البيانات. راجع فصل التوجيهات العامة للمزيد من التفاصيل حول هذا الموضوع.

٧. الاستعانة بمقدمي الخدمات المالية

استخدام البيانات الشخصية

عادة ما يتم توزيع المساعدات النقدية والقسائم بدعم من مزودي الخدمة ، وبالتالي يتم إبرام العقد معهم. في ما يتعلق ببرامج القسائم الشرائية، يشمل مزودو الخدمات تجار السلع والبائعين المحليين والمتاجر الكبرى وتجار الجملة. أما في ما يتعلق ببرامج الدفع بالنقد، فهم مزودو الخدمات المالية مثل المصارف ومشغلي شبكات الهاتف المحمول ووكلاء التحويلات الذين يدعمون الدفع نقدًا. سنركز في هذا الفصل على مبادئ حماية البيانات الخاصة بمزودي الخدمات المالية ولكن يجب أن تنظر كل أنواع مزودي الخدمات في تلك المبادئ. يمكن مراجعة كيفية استخدام مزودي الخدمات بالنموذج3_4M من مجموعة الأدوات المرتبطة بتقديم النقد في حالات الطوارئ.

اعتبارات حماية البيانات

يتطلب التعامل مع مزودي الخدمات المالية مشاركة بيانات المستفيدين الشخصية للتمكن من توزيع الأموال نقدًا. سيركز هذا القسم على القرارات الرئيسية بشأن المشاريع عند العمل مع مزودي الخدمات المالية والاعتبارات المتعلقة بحماية البيانات. ويجب أن تدرج المخاطر المتعلقة بحماية البيانات ومزودي الخدمات المالية في مصفوفة مخاطر تعديل تقييم الائتمان الخاصة ببرنامجك الذي وضع عن طريق مراحل التحليل وتقييم الإجابات في برنامجك. أنظر إلى النموذج 3_4_2M التقييم والنموذج 4_1_3M تحليل الإجابات في مجموعة الأدوات المرتبطة بتقديم النقد في حالات الطوارئ.

قرار المشروع 1: هل يجب أن أستخدم مزود خدمات مالية؟

تقليل استخدام البيانات إلى أدنى حد والضرورة وأمن البيانات

إعادة صياغة مشروع القرار: هل يستطيع مزود الخدمات المالية استخدام بيانات المستفيدين على نحوٍ يلحق الضرر بالمستفيدين؟

عندما تفكر إذا عليك استخدام مزود خدمات مالية في مشروعك، من المهم تحليل ما هي البيانات التي سيطلبها مزودو الخدمات المالية ليقدموا خدماتهم، مما قد ينطوي على طلب معلومات إضافية من المستفيدين لهذا الغرض وتقييم العواقب المحتملة على المستفيدين بعناية عند مشاركة هذه البيانات.[7]

إعرف عميلك وراقب تدقيق القائمة

إن معظم مزودي الخدمات المالية يخضعون لقاعدة اعرف عميلك وذلك يتطلب منهم جمع المعلومات عن العملاء لمنع تبييض الأموال وتمويل الإرهاب وجرائم أخرى. يمكن أن تعتمد كمية المعلومات المطلوبة على القواعد المحلية وتسمح بعض الدول بمرونة أكبر ترتكز على ما تراه مستوى المخاطر في المعاملات. تحتاج الوكالات الإنسانية التي تستخدم مزود الخدمات المالية الالتزام بقواعد إعرف عميلك التي تطلب مشاركة بعض البيانات من المستفيدين.

تُراعى بعض الاعتبارات لضمان مبدأ التقليل إلى أدنى حد والضرورة:

- التحقيق في قوانين إعرف عميلك الخاصة ببلدك وسياق عملها. تحديد البيانات المطلوبة بموجب القانون والتحقق منها مقارنة مع ما يطلبه مزودو الخدمات المالية. قد يوجد سياسات داخلية للسبب الذي يجعل مزودي الخدمات المالية طلب بيانات إضافية خارج نطاق ما يقتضيه القانون، ويجب أن يبرر ذلك ويناقش لضمان مشاركة فقط ما هو ضروري للغاية لتقديم المساعدة.
- في بعض الحالات، يمكن أن تدعو المنظمات الإنسانية إلى متطلبات إعرف عميلك مبسطة أو معدلة (على سبيل المثال، تقليل المتطلبات للناس الذين فقدوا هويتهم أو وضع حد أقصى للمبالغ التي يمكن نقلها للأطراف الثالثة والمستفيدين من خدمة إعرف عميلك أو السماح بالتحويلات النقدية لفترة محدودة). التحقق إذا كان يمكن تقليل البيانات التي تمت مشاركتها مع مزودي الخدمات المالية في هذه الحالات إلى الحد الأدنى.
- إبلاغ المستفيدين وشرح متطلبات إعرف عميلك أو على الأقل إدراج هذه المتطلبات بإشعار الخصوصية الذي يمكن الرجوع إليه في أي وقت.

قد يكون على مزودي الخدمات المالية التزامات بالتحقق من معلومات اعرف عميلك ومشاركة البيانات مع فريق ثالث (على سبيل المثال مع الجهات التنظيمية والسلطات العامة). يمكن أن تشمل عمليات التحقق من إرشادات إعرف عميلك فحص قائمة المستفيدين من قوائم المراقبة وقائمة الجزاءات وقائمة الأشخاص المحددين من السلطات المحلية الذين يمكن أن يكونوا متورطين في نزاع أو أعمال عنف. ويقوم مقدمو الخدمات المالية بذلك بشكل منتظم في حين يقوم آخرون بذلك بناء على طلب الحكومة. وسوف تشير هذه العملية إلى الأفراد الذين يشتبه بتورطهم في أنشطة إجرامية (على سبيل المثال غسل الأموال أوالإرهاب أوالفساد، إلخ) وبالتالي إنهم غير مؤهلين للحصول على النقد. إذا كان يتماشى اسم المستفيد مع أحد من تلك القوائم قد يترتب عليهم عواقب وخيمة. لذلك، يعتبر من المهم للغاية تحليل الدولة وسياق البرنامج. إن الأسئلة النموذجية التي ينبغي التفكير حولها هي:

- هل يوجد تقارير عن اضطهاد سياسي أو عرقي أو ديني من قبل الحكومة؟
- هل يعتبر جزء من السكان المستفيدين معارضين للنظام الحاكم؟
- هل يمكن اعتبار الأحزاب السياسية مجموعات إرهابية؟
- هل يرتبط مزودو الخدمات المالية ارتباطًا وثيقًا بسلطات الحكومة، كأجهزة المخابرات أو الأجهزة الأمنية؟
- إذا كان المستفيدون لاجئين فهل يوجد لدى مزودي الخدمات المالية فرع أو مرفق تخزين في بلد منشأ اللاجئين حيث يمكن أن تطلب السلطات البيانات؟
- هل سيكون هناك قلق بالغ أو خوف من المستفيدين إذا تمت مشاركة بياناتهم بطريقة ما مع الحكومة بسبب هذه الالتزامات؟

إذا شككت في إمكانية استخدام بيانات المستفيدين على نحوٍ غير ملائمٍ فذلك يشكل خطرًا كبيرًا للمستفيدين. وفي ظل هذه الظروف، إذا لم تتمكن من إيجاد طريقة للتعاقد مع مزود خدمات مالية من دون مشاركة بيانات المستفيد، عليك التفكير في خيارات توزيع أخرى

[7] يمكن إيجاد نموذج استبيان لمزودي الخدمات المالية في قسم المراجع الخاص بهذا الدليل.

كالحصول على النقد في الأغلفة أوالقسائم أو دعمًا عينيًّا. ويجب أن يحصل ذلك كجزءٍ من تقييم الخطر في مرحلة الإجابة والتحليل الخاصة ببرنامجك (نموذج 3 من مجموعة الأدوات المرتبطة بتقديم النقد عند حالات الطوارئ) ويجب أن تتضمن هذه المرحلة تحليلًا لما إذا كان ممكنًا أن يؤدي الاضطهاد أو الاستبعاد أو الحساسيات الأخرى إلى جمع معلومات اِعرف عميلك وتبادلها مع اختيار أفضل أساليب التحويل. مراجع أخرى من المنظمة غير الربحية كالب (CaLP): معايير اِعرف عميلك وتوصيات الخصوصية للتحويلات النقدية وورقة نصائح اِعرف عميلك.

أهداف أخرى

نظرًا إلى أن مزودي الخدمات المالية هم عادةً شركات تستهدف الربح، فقد يستخدمون بيانات المستفيدين لغاياتهم الخاصة بما فيها مصالحهم التجارية كالتصنيف من أجل الجدارة الائتمانية والإعلان والتسويق والتحقق من أهلية الحصول على خدمات مالية أخرى. قد يبدو أن تلك النماذج تحمل خطرًا منخفضًا نسبيًا للمستفيدين إلا أنها لا تزال تعتبر خارج نطاق أهداف المساعدة النقدية الإنسانية. يهتم قانون حماية البيانات بحماية الناس من أعمال غير مرغوب فيها تقوم بها المؤسسات الخاصة كإرسال البريد العشوائي.

ويمكن أن يكون الأثر الأكبر الآخر المحتمل من إعادة استخدام مزودي الخدمات المالية البيانات تسديد الديون (مثلًا يدين المستفيد بقرضٍ أو مالٍ من المصرف ويحاول أن المصرف أن يخصم مساعدته المالية ليسدد ما كان مستحقًا) أو زيادة مشاركة البيانات مع الفريق الثالث كمحصلي الديون.

بوجه عام، ينبغي توخي العناية الواجبة بشأن سمعة مزودي الخدمات المالية وأدائها في أثناء عملية المناقصة والتعاقد.[8] وينبغي أيضًا أن تقيد التعاقدات مع مزودي الخدمات المالية المزيد من معالجة البيانات (في أثناء توزيع النقد أو حتى بعده) وتتضمن أمثلة عن أعمال يجب تفاديها، إذا كانت تعرف في وقت التعاقد (انظر إلى القرار بشأن المشروع 3). ينبغي أن يُطلب إلى المستفيدين خلال تنفيذ البرنامج، إبلاغ الجمعية الوطنية بأي حالات استخدام أخرى (أو اشتباه في إساءة استخدام) لبياناتهم من جانب مقدمي الخدمات المالية الذين هم خارج نطاق البرنامج.

قرار المشروع 2: ما هو نوع الحساب الذي يتعين اختياره من أجل توزيع المساعدة النقدية؟

تقليل استخدام البيانات إلى أدنى حد والضرورة وأمن البيانات

إعادة صياغة مشروع القرار: ما هو نوع الحساب الذي يوفر أفضل حماية لمعلومات المستفيدين، عند استخدامه للقيام بعملية توزيع المساعدة النقدية؟

توجد آليات مختلفة لتنفيذ عمليات الدفع النقدي ينبغي النظر فيها، من ضمنها استخدام المصارف و وكالات تحويل الأموال، و موفري خدمات الشبكات المتنقلة، ومكاتب البريد. ومن منظور حماية البيانات ، من المهم النظر في كيفية الحد من مشاركة البيانات الشخصية، بصرف النظر عن آلية الدفع المستخدمة. و يتوقف ذلك أساساً على نوع الحساب المصرفي المستخدم في عملية توزيع المبالغ النقدية. وينبغي مراعاة نوعين من أنواع الحسابات المصرفية هما: إما استخدام حسابات بأسماء الأفراد المستفيدين، أو امتلاك حساب افتراضي تُديره الجمعية الوطنية.

حسابات بأسماء أصحابها

يجوز أن يستخدم البرنامج مباشرة حساب المستفيد، بالتعاون مع مقدم الخدمات المالية، أو فتح حساب نيابة عنه. ويعد استخدام حسابات المستفيدين القائمة أصلاً أقل تداخلاً مع حماية البيانات، مقارنة مع فتح حسابات جديدة، وذلك نظراً إلى العلاقة التعاقدية المسبقة بين مقدم الخدمات المالية والمستفيد، والتي يمكن أن تستفيد منها الجمعية الوطنية في تحقيق أهداف برنامجها. ينبغي إجراء تحليل أكثر دقة بشأن فتح حسابات جديدة من جانب الجمعية الوطنية لصالح فرادى المستفيدين، إذا افترضنا أن ذلك ممكناً، لتحديد المخاطر المحتملة ذات الصلة بحماية البينات. على سبيل المثال، قد يكون هناك سبب محدد لعدم فتح أي من المستفيدين حساب فردي بسبب بعض المخاوف الناجمة عن قاعدة "اعرف عميلك" والتي جرى ذكرها في القسم السابق. ويستلزم فتح حساب نيابة عن شخص آخر، إمعان النظر عند جمع و مشاركة مع مقدم الخدمات المالية، و إدارة الحساب بعد انتهاء البرنامج.

[8] ويمكن الاطلاع على نموذج الاستبيان الخاص بمقدمي الخدمات المالية في قسم المراجع من هذا الدليل الإرشادي.

الحسابات الافتراضية

إن الحسابات الافتراضية عبارة عن حسابات تمتلكها و تديرها المنظمات الإنسانية، والتي تستطيع إنشاء حسابات فرعية لصالح المستفيدين، مما يتيح لهم تلقي المبالغ النقدية. فيما يتعلق بتلك الحسابات، يجري تطبيق قاعدة "اعرف عميلك" على هذه المنظمات الإنسانية، وليس على فرادى المستفيدين. ومن الأمثلة على استخدام الحسابات الافتراضية ما يلي:

- إصدار بطاقات الصراف الآلي مسبقة الدفع حيث ترتبط كل بطاقة بحساب الجمعية الوطنية، و تعطى للأفراد المؤهلين مع تزويدهم برمز التعريف الشخصي الذي يمكنُ استخدامه لسحب النقود
- إصدار شيكات مصرفية للأفراد، يمكن الحصول على مبالغها حتى وإن لم يكن لدى الأفراد المستفيدين حساب في ذلك البنك
- استخدام بطاقات تحديد هوية المشترك التي تعمل على الهواتف المتنقلة والتي تصدرها المنظمة على نطاق محدود، حتى يتسنى للمستفيدين تلقي رسالة نصية قصيرة عبرها تحتوي على رموز المعاملات، يمكن استخدامها لاسترداد الأموال من وكلاء الخدمات النقدية المتنقلة

ومع ذلك، ربما لا تزال هنالك حاجة لمشاركة بيانات المستفيدين مع مقدم الخدمات المالية، لتحديد هوية المستفيد في وقت صرف المبالغ النقدية، غير أن كمية البيانات التي يتم مشاركتها بوجه عام أقل مقارنة مع إنشاء حسابات بأسماء أصحابها (اسمية) وذلك نظراً لعدم تطبيق قاعدة "اعرف عميلك" على الأفراد. من زاوية حماية البيانات، يعتبر هذا الخيار الأفضل، غير أن هناك بعض الاعتبارات التشغيلية أيضاً (على سبيل المثال: قدرة فريق البرنامج على إدارة الحسابات الفرعية، و تسليم القسائم مثل: بطاقات الدفع المسبق من أجل تحصيل المبالغ لصالح أصحابها المستفيدين وربط أرقام الحسابات الفرعية الصحيحة، وتسوية المعاملات بعد الصرف). وترتبط مخاطر إدارة المعاملات والأموال في كثير من الأحيان، بالوكالة. علاوة على ذلك، عند استخدام الحسابات الافتراضية، تستطيع الجمعية الوطنية الاطلاع على البيانات التي تكشف مدى استخدام المستفيدين لهذه الأموال. وتعد هذه البيانات حساسة. ومن أجل احترام خصوصية المستفيدين في هذا الصدد، يُرجى الرجوع إلى الفصل المعنون بالرصد عقب التوزيع لمزيد من التفاصيل حول الخصوصية و عملية الرصد.

قرار المشروع 3: ما الذي يجب أن يتضمنه العقد المبرم مع مقدم الخدمات المالية؟

أمن البيانات

إعادة صياغة مشروع القرار: ما هي الشروط و الأحكام التي ينبغي إدراجها عند التعاقد مع مقدم الخدمات المالية من أجل حماية البيانات الشخصية للمستفيدين؟

أولاً، من المهم تحديد البيانات اللازمة للحصول على خدمات مقدم الخدمات المالية، والتفاوض بشأن تقليل مشاركة البيانات إلى أدنى حد. وعادة ما يشمل ذلك:

- بيانات تحديد الهوية مثل: اسم المستفيد، ورقم بطاقة هوية المستفيد سارية المفعول
- البيانات المطلوبة بشأن قاعدة "اعرف عميلك"، والتي قد تختلف استناداً إلى الأنظمة الوطنية
- البيانات الأخرى اللازمة لتسهيل عملية توزيع الأموال النقدية ، أن وجدت مثل: رقم الهاتف المحمول الخاص بتحويل الأموال عبر الهاتف المحمول، أو رقم الحساب المصرفي، أو الاسم وهوية الشخص المفوض باستلام المبالغ نيابةً عن المستفيد (الوكيل)

ومن المهم أيضاً أن نفهم نوعية البيانات التي قد يقوم مقدم الخدمات المالية بإنشائها و شاركتها معك، بوصفها جزء من المعاملات التي يجري تنفيذها مع المستفيدين. فعلى سبيل المثال، تاريخ وحالة الصرف، وتوقيع المستفيد بعد استلام المبالغ النقدية، والرصيد الحالي في حالة عدم سحب جميع الأموال النقدية من الحساب حتى الآن، و الأماكن التي قد جرى استخدام هذه الأموال فيها (محالات البقالة)، وما إلى ذلك.

ثانياً، ضرورة صياغة عقد، أو اتفاقية الخدمات. حيث ينبغي أن تتضمن هذه الاتفاقية إطار تقديم الخدمات، ونطاق تقديمها وعناصر حماية البيانات. ويوصى بوجود نموذج لهذه الاتفاقية جرت صياغته ومشاركته مسبقاً أثناء عملية طرح العطاءات، ويجري تقييم اعتبارات حماية البيانات كجزءٍ من عملية اختيار مقدم الخدمة.

ويرد فيما يلي بعض الشروط و الأحكام الرئيسية التي ينبغي إدراجها في العقد:

- **تحديد الغرض.** تُستخدم البيانات التي يجري مشاركتها لأغراض البرنامج لا غير (توزيع الأموال النقدية). و لا يجوز استخدام هذه البيانات لأي أغراض أُخرى خارج نطاق البرنامج. وكما ذكر أعلاه قد يكون من المفيد توخي

الصراحة بشأن نوعية البيانات التي ينبغي عدم استخدامها لأغراض (مثل الدعاية و التسويق أو الإعفاء من الديون) أو سرد أمثلة ملموسة في هذا الصدد. يتعين تحديد قائمة نوعية البينات تحت مسمى "غير شاملة".

- **مشاركة البيانات مع الآخرين.** لا يجوز لمقدم الخدمات المالية مشاركة البيانات مع أي أطراف أُخرى دون الحصول على موافقة الجمعية الوطنية. وأيضاً في حالة وجود التزام بمشاركة البيانات (على سبيل المثال مع الجهات الرسمية)، ينبغي إخطار الجمعية الوطنية أولاً.
- **أمن البيانات.** ينبغي تخزين البيانات التي جرت مشاركتها بطريقة آمنة (مثل : الإشارة إلى ضوابط الوصول، والتشفير، وعمليات النسخ الاحتياطي للبيانات).
- **السرية.** ينبغي التعامل مع البيانات التي جرت مشاركتها في إطار من السرية.
- **عدم طلب أي بيانات إضافية من المستفيد.** لا يجوز لمقدم الخدمات المالية طلب الحصول على أي بيانات شخصية أُخرى من المستفيد، تحت مظلة البرنامج. ومثال على ذلك، قد يحتاج المستفيدين إلى إبراز هوياتهم الشخصية للتحقق من الهوية عند المطالبة بالمساعدة النقدية، ومع ذلك لا يجوز لمقدم الخدمات المالية نسخ بطاقة الهوية أو مسحها ضوئياً للحاجة و بالتالي يكون قد حصل على بينات إضافية من المستفيد.
- **الحذف.** ينبغي حذف البيانات التي يجري مشاركتها، من قواعد بيانات مقدم الخدمات المالية عند انتهاء البرنامج، أو حفظها دون الاتصال بشبكة الإنترنت و بشكل آمن لأغراض التدقيق.
- **العواقب المترتبة على إخلال مقدم الخدمات المالي بشروط التعاقد.** ينبغي أن يتضمن العقد صيغة تنص على أن مقدم الخدمات المالية يقر بأن الإخلال بأي شرط من شروط هذا العقد يجوز أن تترتب عليه آثار قانونية قد يلحق الضرر بسمعة جميع الأطراف المعنية، على أقل تقدير. وكذلك الإشارة إلى أهمية تشجيع المستفيدين على إبلاغ الجمعية الوطنية عن أي استخدام لبياناتهم الشخصية غير متصل بالبرنامج، من قبل مقدم الخدمات المالية.

يرجى الإطلاع على قسم المراجع أدناه للحصول على نموذج من الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر بخصوص التعاقد مع مقدم الخدمات المالية. إذ يحتوي على نقاط ذات صلة بحماية البيانات. إذا شعرت بأن هنالك بعض المعلومات لم يرد ذكرها أو ثمة مسألة ما ظهرت في سياق البرنامج و ترغب في تناولها، بالإمكان إضافتها في النموذج الخاص بك.

من الناحية العملية، في كثير من الأحيان يرغب مقدمو الخدمات المالية في استخدام نماذج العقود الخاصة بهم. حسب الموقف الذي يسمح بالتفاوض، حاول استخدام نماذج العقود التي صاغتها الجمعية الوطنية. في حالة الموافقة على استخدام نموذج العقد الخاص بمقدم الخدمات المالية من المستحسن إلقاء نظرة عن كثب و مقارنة عناصر حماية البيانات و مطالبة مقدم الخدمات المالية بتعديلها لضمان حماية بيانات المستفيدين بصورة آمنة. إذا لم يتضمن نموذج مقدم الخدمات المالية على أي نصوص فيما يتعلق بحماية البيانات، فهذه فرصتك لعرض عناصر حماية البيانات التي تعتقد إنها مهمة. تستطيع الجمعية الوطنية استخلاص بنود محددة من نموذج الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر. في حالة عدم موافقة مقدم الخدمات المالية على أي نصوص ذات صلة بحماية البيانات في العقد، يجب أن يكون ذلك بمثابة راية حمراء فيما يتعلق بشروط التعامل مع مقدم الخدمات المالية هذا. يتعين على كل جهة تتمتع بسمعة جيدة أن تهتم الحد الأدنى من معايير حماية البيانات.

و من المعتاد التفاوض على اتفاق إطاري مع أحد مقدمي الخدمات المالية أو أكثر باعتباره جزء من الاستعداد لتقديم المساعدات النقدية، الأمر الذي يوفر خيارات تبعاً للسياق و الاحتياجات. مع ذلك، قد تُظهر البرامج الجديدة حالات جديدة لا تشكل جزءًا من الاتفاق الحالي مع مقدمي الخدمات المالية. إذا كان لديك انطباع بأن مسألة حماية البيانات لم يتم تناولها بشكل كافٍ في الاتفاق الإطاري، لا تتردد في مناقشة ذلك مع مقدم الخدمات المالية أو مديرك من أجل التفاوض على إجراء التعديلات المناسبة. أضحت مسألة حماية البيانات أكثر أهمية خلال السنوات الماضية، غير أن الوعي بها لم يبدأ سوى مؤخراً.

VI. مشاركة البيانات مع الحكومات و المنضمات الإنسانية الأخرى و الجهات المانحة

استخدام البيانات الشخصية

عادة ما تتطلب مبادرات المساعدات النقدية والقسائم التعاون والتنسيق مع طائفة أوسع من أصحاب المصلحة، على غرار الحكومات الوطنية والمنظمات الإنسانية الأخرى (الدولية والمحلية)، و الجهات المانحة. في مثل هذه العلاقات، من الممكن أن تكون هنالك ضرورة إلى مشاركة بيانات المستفيد من جمعية وطنية ما، مع جهات خارجية (وكذلك قد تتلقى الجمعية الوطنية بيانات على ذات المنوال). قد يجري مشاركة البيانات بشكل رسمي من خلال إبرام اتفاقيات بخصوص مشاركتها، أو بطريقة غير رسمية دون اتفاقيات، لا سيما في حالات الطوارئ حيث يعتبر التوقيت عاملاً أساسياً.

رأينا في فصل الاستهداف نماذج على تلقي بيانات المستفيدين من الحكومة و المنظمات الأخرى التي تستجيب لنفس حالة الطوارئ وذلك من أجل إعداد قائمة أولية بأسماء المستفيدين و التحقق من مدى أهلية الأشخاص المدرجين في القائمة. كما أن هذا المستوى من مشاركة البيانات مهم للتنسيق بين مختلف الجهات الفاعلة وذلك لتجنب ازدواجية الجهود و المساعدة المكلفة. أما بالنسبة للجهات الفاعلة، فقد تكون هنالك التزامات بشأن عملية المراجعة و إبداء الشفافية و المساءلة من خلال التأكد من أن المستفيدين الذين تلقوا المساعدات هم أناس حقيقيون، مستحقين بالفعل لهذه المساعدات، وأنهم قد تلقوا استحقاقاتهم النقدية.

اعتبارات حماية البيانات

في هذا القسم سوف يتم التعرف على الاعتبارات الرئيسية المتعلقة بحماية البيانات عند مشاركة البيانات مع الأطراف الخارجية. بشكل عام، عند مشاركة البيانات مع مختلف الأطراف، **من المهم ضمان أن البيانات قد جرى نقلها على نحو آمن عبر وسائل آمنة** (على سبيل المثال الملفات مشفرة, حُفظت في غرف آمنة خاصة بالبيانات) ولا يصل إليها إلا الموظفون المصرح لهم. انظر فصل التوجيهات العامة.

عند نقل بيانات إلى أي دولة أخرى من الضروري تقييم مستوى حماية البيانات في هذه الدولة. إذا كان مستوى الحماية أدنى من معايير الجمعية الوطنية، ينبغي إعادة النظر بشأن نقل البيانات، وإذ كان لا مفر من ذلك، ينبغي التفاوض حول إبرام اتفاقية محددة و تفصيلية بخصوص متطلبات حماية البيانات.

قرار المشروع 1: أي من البيانات التي يجب مشاركتها مع الحكومة؟

أمن البيانات و ضرورة ذلك

إعادة صياغة مشروع القرار: هل من الضروري و الآمن مشاركة البيانات الشخصية مع الحكومة؟

على الرغم من أن الجمعيات الوطنية تعمل بوصفها جهات مساعدة لحكومات بلدانها، غير أنه من الواجب عليها الالتزام بمبادئ الحياد و النزاهة و الاستقلالية عندما يتعلق الأمر بالعمل الإنساني. و مع ذلك، تخضع هذه الجهات أيضاً إلى قوانين وطنية [9]قد تتضمن التزامات قانونية، وبالتالي فهي ملزمة بمشاركة بعض البيانات مع الحكومة. جرت مناقشة بعض المخاطر المتعلقة بحماية البيانات في قسم اعرف عميلك (فيما يتعلق باستخدام مقدمي الخدمات المالية) من حيث إبلاغ عن الأشخاص المعنيين للسلطات (قوائم المراقبة، و قوائم الجزاءات). ويمكن أيضاً أن تتعرض الجمعيات الوطنية إلى ضغوط من جانب السلطات لمشاركة البيانات الشخصية لأغراض أُخرى (مثل مكافحة الإرهاب). وفي ضوء ذلك، تدعو الحاجة إلى إجراء تحليل عند تصميم مبادرة المساعدات النقدية والقسائم - قبل جمع البيانات بفترة - و تقييد هذه المخاطر(من خلال استخدام مصفوفة المخاطر أو إجراء تحليل أكثر تنظيماً باستخدام تقييم تأثير حماية البيانات).

إلى جانب القوانين الوطنية المحددة, ثمة مقاصد أخرى قد تطلب الحكومة من المنظمة فيها مشاركة البيانات مثل:

- **معرفة مبادرات المساعدات النقدية والقسائم.** قد ترغب الحكومات في كثير من الأحيان في الإطلاع على البرامج الإنسانية التي تُنظم على نطاق ولايتها باعتبارها المسؤولة في نهاية المطاف عن أمن و رفاهية المواطنين و السكان في مناطقهم. علاوة على ذلك، في حالة وجود خلافات بين بعض أفراد المجتمع حل سبب عدم إدراجهم في البرنامج فإنهم يقدمون شكاوى أما السلطات. و عادة، ما ترغب السلطات في معرفة الهدف من هذه البرامج و فترتها والفئات المستهدفة و معايير الاستهداف المتفق عليها و النطاق المالي و الاحتياجات الأمنية والمصادر والدعم المطلوبة من السلطات. من الطبيعي تقديم معلومات عامة وافية و بيانات مفصلة (معايير و مناطق الاستهداف و عدد الأشخاص الذين يقدم اليهم الدعم، نسبة كبار المسنين/ الأطفال ، و مبالغ المنح النقدية... وما إلى ذلك)، حتى تتمكن الحكومة من فهم طبيعة البرنامج. في بعض الحالات، قد ترغب هذه السلطات في الاطلاع على القائمة النهائية للمستفيدين الذين جرى استهدافهم. إذا لم تُتاح هذه القائمة لعامة الجمهور بالفعل عن طريق أدوات الاتصال و النشر المجتمعية، من الجيد فهم سبب حاجة السلطات لهذه القائمة، وقد يكون من المطلوب إجراء مفاوضات بشأن الحد من أي بيانات شخصية يجري تقديمها.
- **التنسيق من أجل تجنب ازدواجية المساعدة.** في حالات الطوارئ، عادة ما تقوم الحكومات أيضاً بتنفيذ برامج لدعم المجتمعات المتضررة. في حالة وجود مختلف المنظمات التي تقوم بتقديم المساعدات ، قد تضطلع الحكومة بدور تنسيقي من أجل ضمان عدم ازدواجية المساعدة و دعم هذه المنظمات لتقديم المساعدات في أقرب وقت ممكن. في بعض البلدان و السياقات، يجوز أن تطلب الحكومات بيانات المستفيدين من جميع المنظمات وذلك للتحقق من الازدواجية، وقد يكون من الضروري في بعض الحالات حتى المطالبة بهذه البيانات للتحقق من القائمة قبل شروع المنظمة في توزيع المساعدات. قد يكون القصد من تجنب الازدواجية معقولاً، ويتطلب من الحكومة معرفة أسماء المستفيدين. ومع ذلك، ليس من الضروري مشاركة البيانات الشخصية الأخرى لهذا الغرض. وكذلك، لا تكون هنالك

[9]باستثناء أصحاب الامتيازات و الحصانات.

حاجة عموماً إلى إتاحة إمكانية وصول الحكومة إلى قاعدة البيانات الخاصة بك. فاوض على تقليل مشاركة البيانات مع السلطات لتسهيل التنسيق والتحقق المتكرر مهما امكن.

- **تطبيق الشراكة.** من الممكن أن تكون الجمعية الوطنية شريكة مع الحكومة للتوزيع بالنيابة عن الحكومة. تعتمد الحكومة على برامج الجمعيات الوطنية والموزعين في مدى وصولهم وطاقاتهم. في مثل هذه الشراكات, تُنشأ شراكة رسمية. عند التفاوض بخصوص مثل هذه الاتفاقيات، يُرجى مراعاة حماية البيانات وأفضل الممارسات.

بغض النظر عن الهدف الرسمي، لا بدّ من مراعاة مسألتين محتملتين. أولًا، في حالات معينة، من المحتمل إعادة استخدام البيانات الشخصية عند مشاركتها لأغراض أخرى. ثانيًا، حتى عندما تشارك مقدارًا محدودًا للغاية من البيانات الشخصية، يمكن الجمع بين هذه البيانات والبيانات الأخرى التي تحتفظ بها الحكومة فعلًا. من الصعوبة التنبؤ بالعواقب التي قد يترتب على ذلك بالنسبة إلى المستفيدين. وللحد من هذين الخطرين، قد يكون هناك اختيار لتقديم نسخة مطبوعة فقط من قائمة المستفيدين. تعد البيانات غير الرقمية أكثر صعوبة في إعادة استخدامها. من الأفضل إظهار القائمة فقط في الاجتماع وإعادة أخذ النسخة المطبوعة معك حالًا. يعتمد ذلك على السياق الذي ستقبل فيه الحكومة مثل هذه الطريقة، لكن تتلخص الفكرة هنا في محاولة الخيارات للحد من مشاركة البيانات.

حيث ينبغي تقديم البيانات الشخصية إلى الحكومة، تذكّر ما يلي:

- كن واضحًا فيما يتعلق بهدف مشاركة البيانات والعواقب أو المخاطر المحتملة بالنسبة إلى المستفيدين التقليل منها حيث أمكن وتحديد الأساس القانوني.
- إن أمكن وضع اتفاق لمشاركة البيانات. سيحدد مثل هذا الاتفاق رسميًا الغرض من مشاركة البيانات الشخصية وسيحصر استخدام البيانات لهذا الغرض بالذات. يتطلب هذا أيضًا من المُستفيد المحافظة على سلامة البيانات الشخصية وحفظها لفترة لا تزيد عن الضروري. الرجوع إلى نموذج مقدمي الخدمات المالية التابع للاتحاد الدولي لجمعيات الصليب الأحمر[10] للإرشاد العام. تتمتع الجمعية الوطنية بدور مساهم مع الحكومة والذي قد يكون مهمًا في التفاوض بشأن الاتفاقيات المتعلقة بمشاركة البيانات.
- إعلام المستفيدين أنه سيتم مشاركة البيانات مع الحكومة وشرح سبب ذلك. كما كن واضحًا مع أي دوائر حكومية سيتم مشاركة البيانات بشكل أساسي. قد يمنع هذا بعض المستفيدين من مشاركة بياناتهم وينبغي أن يعالجه البرنامج.

قرار المشروع 2: ما هي البيانات التي ينبغي مشاركتها مع المنظمات غير الحكومية الأخرى؟

تقليل استخدام البيانات إلى أدنى حد والضرورة وأمن البيانات

إعادة صياغة مشروع القرار: هل من الضروري مشاركة البيانات الشخصية مع المنظمات غير الحكومية الأخرى وهل يمكن القيام بذلك بسلامة/وأمان؟

قد يكون من الضروري مشاركة المعلومات مع المنظمات غير الحكومية الأخرى في سياقات محددة. أدناه بعض الأمثلة والاعتبارات الجوهرية لحماية البيانات التي ينبغي أن تشمل الأسئلة التالية:

- هل من مصلحة المستفيدين مشاركة بياناتهم؟
- هل ستعرض المستفيدين إلى الخطر؟
- هل يمكنني التأكد أنه ستبقى المعلومات سرية ولن يتم مشاركتها مع الآخرين دون موافقتي؟
- هل لدى المنظمة الأخرى معايير كافية لحماية البيانات؟

مهما كانت الحالة، ستمثل مشاركة أكثر من الأسماء وتفاصيل الاتصال مشكلة. تميل المؤشرات الهشية لأن تكون خاصة جدًا، وحيثما أمكن، ينبغي أن يتاح للمستفيدين أنفسهم إمكانية تقرير مع مَنْ يرغبون مشاركة هذه البيانات.

من أجل التنسيق. تلعبُ مشاركة البيانات دورًا حيث تقدم عدة جهات إنسانية فاعلة معًا مساعدة في مجالي النقد والقسائم، ومن الضروري العمل على نحوٍ منسق (مثل: مجموعات العمل المحلية النقدية). مع تشغيل البرامج المختلفة في نفس الوقت، من المهم تجنب التكرار والتأكد من عدم حدوث الضرر بسبب إجراءات الجهات الفاعلة المتعددة. تتناول بعض الجهود التنسيقية إلى مواءمة مبالغ المنح النقدية واستهداف المعايير والأساليب. بغض النظر عن هذه النوايا المعقولة، من المستحسن أن نراقب بشكل حاسم وأن ننظر فيما إذا كان من الضروري حقًا مشاركة البيانات الشخصية - ولأي مدى- من أجل تنسيق العمل. غالبًا ما يعدُ مشاركة المعلومات العامة والبيانات المجمعة خيارًا جيدًا (المعايير المستهدفة والأماكن الجغرافية المستهدفة وعدد الأشخاص المدعومين والنسبة المئوية للبالغين أو الأطفال ومبالغ المنح النقدية، وما إلى ذلك). حتى حيثما يكون الغرض تجنب التكرار، ليس من الضروري تلقائيًا مقارنة قوائم المستفيدين. استنادًا إلى السياق، يمكن تجنب التكرار عن طريق تخصيص مجالات مختلفة من النشاط (قرية أ/قرية ب) أو

[10] يمكن إيجاد نموذج العقد مع مقدمي الخدمات المالية في القسم المرجعي من هذا الإرشاد.

استهداف مجموعات مختلفة (النساء الحوامل/كبار السن). حيث تستخلص بحتمية مشاركة بيانات المستفيدين، فإن حماية البيانات تتطلبُ منك تحديد مقدار البيانات المشاركة إلى أقصى حد. مثلًا، قد يكون كافيًا مقارنة قوائم المستفيدين المطبوعة في اجتماع مشترك مع المنظمات غير الحكومية الأخرى. ويعد هذا أقل خطورة من منح المنظمات غير الحكومية الوصول إلى قاعدة بياناتك أو إرسال القوائم عبر البريد الإلكتروني.

الاستفادة من الخبرات والوصول إلى داخل المجتمع المحلي. في حالات معينة، قد يكون لدى منظمة غير حكومية واحدة معرفة متخصصة بخصوص قطاع أو مجموعات داخل المجتمع المحلي (مثلًا: المجموعات التي تستهدف النساء والأطفال الضعفاء). قد تحتاج الجمعية الوطنية هنا إلى التعاون مع مثل هذه المنظمة غير الحكومية للاستفادة من خبراتها أو معرفتها للمجتمع المحلي. في كثيرٍ من الأحيان، تعتمد المنظمات غير الحكومية الأخرى على الجمعية الوطنية بسبب حضورهم الشعبي في العديد من المجتمعات وفي أوقات وجود الجهة الإنسانية الفاعلة فقط هنا.

كما قد يكون هناك حالات حيث ترغب فيها منظمة غير حكومية أخرى في تأسيس مشروعها الخاص استنادًا إلى مجموعة بياناتك بشأن المستفيدين المتواجدة مسبقًا. ويعد هذا أمرًا عمليًا ويوفر الوقت في جمع البيانات. مع ذلك، يعني هذا زيادة استخدام البيانات الشخصية التي قد لا تتوافق مع الغرض الأصلي من جمع البيانات. حتى وإن يبدو هذا أكثر ملائمة من وجهة نظر المستفيدين لأنهم قد يتلقون المزيد من المساعدة، ولا تزال مشاركة البيانات هنا أمرًا استثنائيًا وليس القاعدة، وينصح توخي الحذر.

تطبيق الشراكة. كما تعد مشاركة البيانات أمرًا مهمًا في تنفيذ الشراكة حيث قد تبرمُ منظمة واحدة عقدًا لتقديم المعونة/الخدمات بالنيابة عن منظمة أخرى أو مشاركة المسؤوليات في تنفيذ المساعدة في مجالي النقد والقسائم. مثلًا، تعمل وكالة الأمم المتحدة للاجئين مع العديد من المنظمات غير الحكومية في تقديم الخدمات إلى اللاجئين. في مثل هذه الشراكات، عادةً ما يجري التفاوض حول مشاركة البيانات وإدراجها في العقد أو الاتفاقية. عند إجراء مثل هذه المفاوضات، من المهم تقييم المخاطر التي يتعرض لها المستفيدين عندما تشارك البيانات ويتم تناولها عن طريق الشركاء، فضلًا عن الأدوار والمسؤوليات المناطة إلى الشركاء والمسؤوليات المشتركة في حماية البيانات. من المحتمل أن تُملي الوكالة الرائدة معايير لحماية البيانات، مع ذلك، لو وجد تقييمك للمخاطر ثغرات أو كنت تعتقد أن هناك حاجة إلى تعزيز بنود معينة، فلا تتردد في التواصل مع مديرك و/أو مناقشة ذلك مع الفريق القانوني داخل جمعيتك الوطنية من أجل معالجة الأمر في إجراءات التفاوض. على سبيل المثال، لو جمعت جمعيتك الوطنية بيانات من المستفيدين، فهل أنت بحاجة إلى تسليمها بالكامل إلى الشريك الرائد أو يمكنك تقليل البيانات إلى أدنى حد ممكن لما هو أساسي للوفاء بمسؤولياتك في الشراكة؟ لو كان لديك برامج متوازية من المساعدة في مجالي النقد والقسائم تستهدف نفس المستفيدين بموجب تنفيذ اتفاقية الشراكة، كيف يمكنك ضمان الفصل للوصول إلى الشركاء من أجل أمور تقع خارج نطاق الاتفاقية؟

المنصة المشتركة. وهناك بعض المبادرات لوضع منهاج عمل مشترك من حيث تبادل بيانات المستفيدين واحتمالية استخدام عدة منظمات تشارك نفس آلية الدفع. قد يتضمن هذا امتلاك قاعدة بيانات واحدة أو آلية للوصول إلى قابلية التشغيل البيني لأنظمة البيانات التي تمتلكها الوكالات كي تشارك وتكشف عن المجموعة المتفق عليها من البيانات المفيدة. وتهدف هذه المنصة إلى تحسين التنسيق والتعاون فيما بين الجهات الفاعلة في المجال الإنساني، وقد تحظى بتأييد بعض المانحين لأنها قد تحسن الكفاءات. وهناك نُهُج مختلفة لإقامة مثل هذه المنصات المشتركة، وينبغي للجمعية الوطنية أن تقيّم مرة أخرى احتياجات المستفيدين ومخاطرهم قبل مكاسب الكفاءة التي تحققها المنظمات. بعض الأسئلة التي ينبغي أن تؤخذ بعين الاعتبار:

- هل هذه المنصة ضرورية تماماً لكي تقدم الجمعية الوطنية المساعدة النقدية؟ وهناك طرق مختلفة للتنسيق والتعاون مع المنظمات غير الحكومية الأخرى قد لا تتطلب الوصول المباشر إلى بيانات المستفيدين.
- وما هي البيانات المطلوبة للمشاركة في المنصة المشتركة وهل يمكن التقليل منها إلى أدنى حد؟
- كيف ينبغي إبلاغ المستفيدين عند استخدام بياناتهم من قبل الوكالات الأخرى؟ ومن يجب أن يخبرهم؟
- وبمجرد أن يتم تقاسم البيانات عبر المنصة المشتركة (أي تتمكن الوكالات الأخرى من الوصول إلى بياناتك) كيف يضمن الشركاء استخدام البيانات للغرض المتفق عليه؟
- وما هي السمات الأمنية للمنصة التي تكفل حصول الأفراد المأذون لهم فقط على البيانات؟
- ما هي إدارة وصول مختلف المنظمات غير الحكومية إلى البيانات؟ وكلما زاد عدد المنظمات غير الحكومية المنضمة إليها أصبح إدارتها أكثر صعوبة. ولا سيما عندما تقرر إحدى المنظمات التوقف عن المشاركة في المنهاج المشترك، كيف يمكن استخدام البيانات التي تتقاسمها في المستقبل؟
- فأين سيتم تخزين البيانات وهل يثير هذا الموقع (خارج البلد المستهدف على سبيل المثال) قضايا تتعلق بالامتثال لحماية البيانات؟

وإذا كان القرار يتعلق بتشارك بيانات مع المنظمات الغير حكومية الأخرى، فمن المهم أولاً التوصل إلى اتفاق بخصوص ذلك. وينبغي تحديد الأساس القانوني لمعالجة تلك البيانات. وحيثما يتم تقاسم البيانات من خلال منصة مشتركة، يجب أن يكون هذا الاتفاق أكثر صلابة، مع تحديد معايير قوية لحماية البيانات ونطاقها وأدوار ومسؤوليات الشركاء المشاركين. ويوصى بإشراك خبراء تكنولوجيا المعلومات والخبراء القانونيين في التفاوض على الاتفاق من أجل وضع منهاج عمل مشترك لضمان مستوى كاف من الحماية. ثانيا، ينبغي إبلاغ المستفيدين بأنه سيتم تقاسم البيانات مع الوكالات الأخرى. وإذا لم يكن الغرض من تبادل البيانات وقت الجمع أو التسجيل،

فسيكون من الصعب عليكم إبلاغ كل فرد. وفي هذه الحالة، ينبغي أن تكون المنظمة غير الحكومية الأخرى مسؤولة عن استخدام البيانات التي تتقاسمها لإبلاغ هؤلاء المستفيدين. ومن المستحسن توضيح ذلك في اتفاق تقاسم البيانات.

قرار المشروع 3: أي من البيانات التي يجب مشاركتها مع المانحين؟

تقليل استخدام البيانات إلى أدنى حد والضرورة وأمن البيانات

إعادة صياغة مشروع القرار: هل من الضروري و الآمن مشاركة البيانات الشخصية مع المانحين؟

من المهم بالنسبة للمانحين ضمان المساءلة والشفافية في أنشطتهم التمويلية، ولذلك قد يطلبون منكم تقاسم بعض البيانات حول المستفيدين. إنه مهم أيضا أن نفكر في المخاطر المحتملة بالنسبة لخصوصية المستفيدين وأن ننظر في الخيارات الكفيلة بالحد من كمية البيانات المشتركة.

هناك غرضان رئيسيان بالنسبة للجهات المانحة لطلب واستخدام بيانات المستفيدين:

- **الحصول على فهم للبرنامج ورصد الحالة.** ويريد المانح عادة أن يفهم الظروف في الميدان وكيفية استجابة فريق البرنامج. وهنا، يكفي عادة توفير المعلومات العامة والبيانات المجمعة (المعايير المستهدفة، والمناطق، وعدد الأشخاص المدعومين، والنسبة المئوية من كبار السن/الأطفال، ومبلغ المنحة النقدية، وما إلى ذلك). وليس من الضروري عادة تبادل تفاصيل أخرى كالأسماء والبيانات الشخصية . وقد يهتم المانح أيضا بمعرفة كيفية إنفاق المستفيدين للأموال التي يتلقونها. [11] ومرة أخرى، ينبغي أن تكفي البيانات المجمعة (على سبيل المثال، النسبة المئوية من الناس الذين أنفقوا المال على الغذاء وغيره من السلع الأساسية، والنسبة المئوية من الناس الذين احتفظوا بالمال لفترة أطول من أسبوع واحد، وما إلى ذلك).
- **لتحقيق متطلبات مراجعة الحسابات.** وكثيرا ما يحتاج المانح إلى بيانات من المستفيدين للوفاء بمتطلباته في مجال مراجعة الحسابات. ويجب على الجهات المانحة أن تتأكد من أن الأموال الممنوحة تستخدم فعلا للغرض المقصود. وهناك مراجعات أخرى تتحقق فيما إذا كان المستفيدون أشخاصاً حقيقيين، وأنهم استوفوا المعايير المتفق عليها، وأنهم تلقوا بالفعل المساعدة النقدية (إثبات وصل الاستلام). وبالنسبة لهذه الأنشطة ذات الصلة بمراجعة الحسابات، هناك خيارات مختلفة لحماية خصوصية المستفيدين من خصوصية حماية الخيارات:

وعند **مشاركة قائمة** لإجراء عمليات التحقق، يمكن حصر البيانات المدرجة في الحد الأدنى المطلوب، ويمكن استخدام الهوية المرجعية الفريدة بدلا من كشف أسماء المستفيدين. فعلى سبيل المثال، لإثبات الاستلام، ينبغي أن يكون تاريخ والتوقيع الخاص بالاستلام واضحاً. وفي بعض الحالات، قد لا يكون الاسم ضروريا ما دامت هوية المستفيد موجودة. وإذا تم جمع التوقيعات على الورق التي تحتوي على معلومات أكثر مما يلزم، ينبغي تنقيح الأعمدة المعنية أو إزالتها أو إهمالها قبل إرسالها إلى الجهة المانحة لزيادة حماية البيانات.

وثمة نهج آخر يتمثل في إتاحة إمكانية الوصول إلى قاعدة البيانات أو الوثائق **خلال وقت محدود وفي وضعية القراءة فقط** التي يمكن لمراجعي الحسابات أن يجروا فحوصهم في مواقعهم على وجه التحديد. بحيث يمكن لمراجعي حسابات المانحين التحقق من البيانات أو الوثائق ذات الصلة شخصياً معكم ، دون تنزيل أو أخذ أي بيانات. ويمكنك أن تناقش مسبقاً مع الجهة المانحة المعلومات اللازمة والأساليب اللازمة لإجراء هذه التحقيقات. وينبغي إدراج مشاركة البيانات مع المانحين في العقد أو الاتفاق معهم حول مشاركة بياناتهم.[12] وينبغي تحديد الأساس القانوني لمشاركة البيانات وإطلاع المستفيدين على ما يعتزم تقاسمه من بيانات مع المانحين.

VII. رصد ما بعد التوزيع

استخدام البيانات الشخصية

ولفهم ما إذا كان يجري تحقيق أهداف البرنامج، يلزم وضع استراتيجية للرصد والتقييم. ويتمثل جزء من هذه الاستراتيجية في تحديد المؤشرات اللازمة لتحديد النواتج والنتائج والأثر، فضلا عن منهجية الحصول على هذه المؤشرات وتحليلها. وهناك أنواع مختلفة من الرصد، بما في ذلك مراقبة السوق، ومراقبة خط الأساس، ومراقبة المدفوعات النقدية (باستخدام إحصائيات الخروج عادة)، ومراقبة

[11] يرجى ملاحظة أنه لا ينبغي جمع هذا النوع من المعلومات تلقائياً. ويجب أن يكون هناك سبب مشروع لجمع المعلومات عن مشتريات المستفيدين. وقبل جمع هذه المعلومات، التي قد تكشف عن معلومات حساسة عن المستفيدين، يجري استعراض لحماية البيانات. انظر الفصل المتعلق بما بعد المراقبة.

[12] ومن المهم النظر في مسائل مثل متطلبات مراجعة الحسابات في مرحلة التفاوض بشأن العقود.

ما بعد التوزيع. سنركز في هذا القسم على مراقبة ما بعد التوزيع (PDM). وللاطلاع على مزيد من التفاصيل عن الرصد والتقييم، انظر الوحدة 2_5M لرصد برامج مجموعة أدوات اللجنة.

وبالنسبة للمنظمات الإنسانية والجهات المانحة، من المهم معرفة كيف ومتى يستخدم المستفيدون الأموال التي يتلقونها. عادة ما يتم إجراء عملية إدارة البيانات الشخصية بعد أسابيع قليلة من التوزيع النقدي للسماح للمستفيدين باستخدام الأموال التي تلقوها. تُعد عملية إدارة البيانات الشخصية مفيدة لتقييم جودة البرنامج ولتحسين البرامج النقدية المستقبلية واستخدام البيانات الشخصية على الأرجح. بحسب البرنامج قد يكون هناك زيارات متعددة للمستفيدين لرصد التقدم (على سبيل المثال: بناء المأوى كنوع من التعافي) حيث سيتم تتبع قواعد البيانات المختلفة بمرور الوقت.

اعتبارات حماية البيانات

قد تشير كلمة «مراقبة» بأن المستفيدين يمكن التحكم بهم بطريقة معينة، وبأن سلوكهم يمكن تحليله. ولكن في الحقيقة، ليس المستفيدون من يتم التحكم بهم، بل تتم مراقبة البرنامج وفعاليته. ومع ذلك، هذا لا يعني أن مراقبة البرنامج لن يكون لها أثر على المستفيد. وبذلك فإن خصوصية المستفيدين يجب أن تؤخذ بعين الاعتبار.

يرجى الملاحظة: بأن قرارات المشروع الواردة في هذا الفصل ستركز على إدارة البيانات الشخصية. بالنسبة إلى مراقبة خط الأساس والتحويل، فإن الجانب الرئيسي هو تقليل البيانات إلى الحد الضروري فقط. عند جمع البيانات من المستفيدين فإنه من الضروري التفكير في البيانات الضرورية حقا في سياق مراقبة البرنامج. عند استخدام نماذج موحدة فلا بد من تكييفها مع السياق عن طريق تنقيح الأسئلة الغير ضرورية. ارجع إلى فصول الاستهداف وتسجيل المستفيدين. هناك طريقة أخرى موصى بها لزيادة مستوى حماية البيانات في مراقبة خط الأساس والتحويل وهي إزالة التعريف المباشر للمستفيدين (على سبيل المثال، الأسماء والمعرفات الشخصية).

قرار المشروع 1: ما هي البيانات الشخصية التي يجب أن أجمعها في عملية المراقبة؟

تقليل البيانات، ضرورة

إعادة صياغة مشروع القرار: كيف يمكنني الحد من استخدام البيانات الشخصية في عملية المراقبة؟

بالاعتماد على السياق، يمكن أن تتم المراقبة بطرق مختلفة. سنتطرق هنا في إدارة البيانات الشخصية لعمليات النقل المشروطة وغير المشروطة واعتبارات حماية البيانات.

الشروط والقيود

قد يكون لبرنامج المساعدات النقدية والقسائم *شروط معينة* (شرط أساسي يجب على المستفيدين الوفاء به قبل تلقي النقود مثل الذهاب إلى المدرسة، أو تعزيز الصحة، أو ورشة عمل سبل العيش) أو *قيود* (تتطلب من المستفيدين استخدام المساعدة لعناصر أو خدمات محددة أو تحقيق مخرجات مثل إصلاح المأوى أو بدء سبل العيش). إن الهدف من المراقبة هو التحقق مما إذا كانت الشروط ما زالت مستوفاة وبأن القيود يتم احترامها بمرور الوقت. أحد الاعتبارات الرئيسية هو خصوصية المستفيدين. ويمكن إنجاز ذلك عبر تقليل كمية المعلومات التي يتم جمعها إلى ما هو ضروري للغاية. بالإضافة إلى ذلك، فإنه من المفيد وضع فترات زمنية منطقية للمراقبة و تقليل عدد الأشخاص المشاركين بمراقبة نفس المستفيدين. أيضاً، قم بالحد من الوصول إلى البيانات المصنفة التي قد يستخدمها مختلف أصحاب المصلحة الذين يساعدون أو يشاركون في عملية المراقبة.

مثال:

في سياق البرنامج، يجب على المستفيدين استخدام مساعدتهم لبناء مأوى بعد إعصار مدمر. قرر فريق البرنامج أنهم سيزورون كل مستفيد بعد أسبوع واحد ومرة أخرى بعد ثلاثة أسابيع لمعرفة مدى التقدم في إعادة بناء المأوى. سيسأل الفريق عن المواد التي تم شراؤها باستخدام المساعدة النقدية ويتحقق بصرياً من حالة المأوى. لن يطلبوا من المستفيد ملء نماذج مطولة عن ظروفهم المعيشية العامة أو التقاط صورة للبناء. كما قرر فريق البرنامج أن يكون لديه فريقان منفصلان للمراقبة يقومان بتغطية مناطق جغرافية مختلفة. ستقوم نفس الفرق بمراقبة نفس الأسر بعد ثلاثة أسابيع لضمان اتساق المراقبة حيث لم يتم التقاط الصور، ويمكن للموظفين نفسهم التحقق من التقدم المحرز في البناء.

غير مشروط وغير مقيد

عندما يتم تقديم النقد للمستفيدين من أجل إنفاقه على احتياجاتهم الخاصة وليس لسلعة أو نشاط محدد مسبقاً، فقد تكون المراقبة مختلفة. ستظل هناك حاجة إلى بيانات المستفيدين لمعرفة (بشكل عام، على سبيل المثال حسب الفئة) كيف أنفقوا استحقاقاتهم وما إذا كانت أهداف البرنامج قد تحققت. القصد هنا ليس مراقبة المستفيد الفردي، ولكن لفهم فعالية البرنامج. يعتبر السلوك العام للمستفيدين المشاركين مؤشراً مهماً لتقييم ما إذا كانت معايير الاستهداف ومقدار النقد المقدم مناسبين.

تتمثل إحدى طرق المراقبة النموذجية في إنشاء مناقشات مجموعة التركيز مع عينة من المستفيدين وغير المستفيدين من المجتمع. النقاش الشفوي مع هؤلاء الأشخاص يتركز حول المشروع بشكل عام. حيث أنهم يُسألون عادةً عن رأيهم في المشروع (معايير الاستهداف، وتأثيرات المشروع، وما إلى ذلك.) بالإضافة إلى ذلك فإنهم مدعوون لتبادل خبراتهم عن كيفية استخدام الأموال. من منظور حماية البيانات، تكون المناقشات الشفوية على هذا النحو أقل إشكالية من الجمع الرسمي للمعلومات في شكل ورقي أو رقمي. ومع ذلك، ينبغي النظر بعناية في كيفية تسجيل مناقشات مجموعات التركيز. يمكن أن تتعارض تسجيلات الفيديو والتسجيلات الصوتية مع خصوصية المستفيدين. بشكل عام يفضل أخذ محضر للاجتماع. على الأغلب أن هذا سيسهل الأمر على المشتركين للتعبير عن آرائهم وتجاربهم. عند تدوين ملاحظات الاجتماع، هناك خيارات لزيادة مستوى الخصوصية. يجدر التفكير في قصر ملاحظاتك على:

- نقاط المناقشة العامة - بدلاً من انتقاء الأفراد وتعليقاتهم الخاصة
- عدد المشاركين وخصائصهم الرئيسية التي تجعلهم عينات جيدة (العمر والجنس ومنطقة المعيشة) - بدلاً من تسجيل أسمائهم الكاملة

قد لا تبقى التعليقات مجهولة تماماً. سيعرف الأشخاص المشاركون في المناقشة من قال ماذا. ومع ذلك، بالنسبة للأشخاص الذين يرجعون إلى ملاحظات الاجتماع لاحقاً، سيكون من الصعب تحديد شخص واحد وراء تعليق معين. بالطبع، يعتمد الأمر على السياق فيما إذا كانت هذه المعلومات المحدودة ستكون كافية لأغراض المراقبة.

طريقة أخرى للمراقبة هي عمل مقابلات مع مجموعة من المستفيدين. هذا يتم بالعادة عبر نموذج استبيان. من الضروري التحقق من هوية الشخص الذي تتم مقابلته للتأكد من أنه الشخص الصحيح وبأنه بالطبع قد تلقى المساعدة المالية. ولكن قد لا تكون معلومات الهوية هذه ضرورية للتخزين، لذلك يمكن الحفاظ على مستوى معين من إخفاء الهوية. سيعرف القائم بإجراء المقابلة هوية المستفيد، ولكن البيانات التي يتم إنتاجها بعد إكمال الاستبيان ستتمتع بحماية أكبر من الآخرين الذين يرجعون إلى البيانات.

مثال:

يطلب فريق البرنامج عينة من المستفيدين للمشاركة في إدارة البيانات الشخصية لمعرفة كيفية استخدام المساعدة النقدية.[13] يتحقق الفريق من معرفات المشاركين ولكنه لا يدون أسماءهم وهوياتهم في نموذج الاستبيان. في الاستبيان، كان المستفيدون صريحين بشأن عدم رضاهم بشأن التحصيل لأنه تطلب منهم السفر بعيداً للوصول إلى وكيل الأموال، وكانت هناك مشكلات في السيولة مع وكيل الأموال، وأشار المستفيدون إلى أنه كان من الأفضل لتقي مساعدة عينية بدلاً من النقد. احتراما لخصوصيتهم، أتاحت نزاهة فريق برنامج العمل لأن يتعلم ويتكيف بالنسبة للدفعة النقدية القادمة، بدلاً من القول تظاهراً بأنهم راضون وذلك خوفاً من عدم استلامهم للنقد بعد الآن.

في حالة عدم التمكن من إبقاء هوية المستفيد مجهولة في الاستبيانات، يصبح مهما أن تقلص الأسئلة إلى أدنى حد لازم. تنحى الصيغ النموذجية إلى شمول نطاق واسع من الأسئلة التي تغطي مختلف السيناريوهات ("نهج واحد يناسب الجميع"). وكما تم توضيحه في الفصل الخاص بالتسجيل، ينبغي أن تصمم الصيغ النموذجية الموحدة بما يلائم الظروف الخاصة وبحسب الحاجة. ينبغي شطب أو حذف الأسئلة غير الضرورية.

حاول إيجاد خيارات تتجنب استخدام البيانات الشخصية. في حالة استخدام المعلومات لأغراض الرقابة ينبغي حينئذ التحقق من الأسس الشرعية للرقابة وإعلام المستفيد عن كيفية تداول بياناته ضمن نطاق الرقابة.

[13] يرجى الانتباه إلى أنه ينبغي أن يعطي المستفيدون المعلومات طوعاً، إذ لا يمكن إرغامهم. ينبغي أن يوضح لهم بأن مشاركتهم سوف لن تؤثر على المدفوعات الحالية ولا المستقبلية ولهم الحرية في رفض المشاركة.

قرار المشروع 2: ماهي بيانات المستفيدين التي يمكن لمقدمي الخدمات المالية أن يعطوها لي لكي أراقب البرنامج الخاص بي؟

تقليص البيانات وتحديدها بأدنى ما تقتضيه الضرورة والمحافظة على سريتها

إعادة صياغة مشروع القرار: ماهي البيانات التي يمكن لمقدمي الخدمات المالية أن يعطوها لي، لأغراض الرقابة، دون انتهاك خصوصية المستفيدين؟

عندما تستخدم البرامج النقدية مقدمي الخدمات المالية، يمكن أن تتوفر لمقدمي الخدمات هؤلاء بيانات عن المستفيدين قد تكون مفيدة في عملية الرقابة. تبعاً لمقدم الخدمات المالية فإن بعض البيانات التي قد تتوفر لديهم يمكن أن تتضمن: زمان ومكان سحب النقد (ماكينة الصراف الآلي أو عن طريق وكلاء الصيرفة)، وهل استخدمت الأموال للشراء من مرافق معينة (كأن تكون محل بقالة أو مخزن لبيع الخمور) بالإضافة إلى التوقيع كإثبات للاستلام. قد يساعد الحصول على مثل هذه البيانات في تعجيل العملية والحصول على معلومات دقيقة عن عملية الرقابة، غير أنه، ومن وجهة النظر الخاصة بحماية البيانات، فإن هذا النهج قد يشكل مخاطر معينة. البيانات المتعلقة بالمدفوعات والمشتريات قد تكون حساسة جداً. إن جمع مثل هذه البيانات من مصدر غير مباشر(مقدم الخدمات المالية) بدلاً من تحصيلها من المستفيدين مباشرة قد ينظر إليه كتدخل في خصوصيتهم.

الحسابات الشخصية للمستفيدين

عندما يتم الصرف من خلال الحسابات الشخصية (المصرف/الهاتف المحمول) للمستفيدين، فإن الجمعية الوطنية لا تتمكن من الوصول إلى هذه الحسابات تلقائياً. غير أنه باستطاعة مقدم الخدمات المالية تتبع مسار حركات الحسابات وقد يكون مستعداً لتبادل بيانات المدفوعات المعنية معك. عليه، يصبح السؤال، هل لهذا صلة بالموضوع وماهو اللازم لغرض الرقابة؟ قد تريد أن تفهم متى وكيف تم استخدام الأموال. غير أن محور الرقابة لا ينصب على الفرد المستفيد وإنما ينصب على السلوك العمومي لمجمل المستفيدين. وعليه فإنه، اعتيادياً، يمكن أن تكتفي بالحصول على القيم الإجمالية للمدفوعات. على سبيل المثال، يمكن لمقدم الخدمات المالية أن يعلمك عن:

- النسبة المئوية من المستفيدين الذين صرفوا أموالهم في الأسبوع الأول
- النسبة المئوية من المستفيدين الذين استخدموا أموالهم في مرفق معين كأن يكون سوق مركزي أو صيدلية
- معدل الفترة الزمنية التي يستخدم خلالها المستفيدون أموالهم بأكملها
- المناطق التي تصرف فيها الأموال على نحو أسرع
- المواقع النسبية لوكلاء الصيرفة ومن منهم كان يصرف أكثر من غيرهم

تبعاً لسياق برنامجك، يمكنك الاتفاق مع مقدم الخدمات المالية على ماهية المعلومات التي عليهم توفيرها، مع مراعاة مبدأ الحد الأدنى اللازم من البيانات.

مثال:

يتولى برنامج معين لصرف النقد باستخدام البطاقات المدفوعة مسبقاً حيث يستطيع المستفيدون استخدامها للشراء من المخازن والمرافق التي تتقبل بطاقات الائتمان (ماستر كارد) أو للسحب عن طريق ماكينة الصراف الآلي. تود الجمعية الوطنية أن تعرف أصناف السلع التي كان النقد يستخدم لاقتنائها والتحقق من مقدم الخدمات المالية فيما إذا كان باستطاعتهم توفير هذه المعلومات للجمعية. يطلب فريق برنامج العمل، وبالتحديد، البيانات التجميعية والتصاوير البيانية لمعرفة (1) فيما إذا كان النقد يستخدم أكثر للسحب عن طريق ماكينة الصراف الآلي مقابل الشراء من المخازن، (2) النسبة المئوية من المستفيدين الذين لم يستخدموا معونتهم النقدية بعد، و(3) فئات المرافق التي استخدمت فيها البطاقات (على سبيل المثال، غذاء، دواء، خدمات). يقوم مقدم الخدمات المالية بتوفير ما يقتصر على البيانات التجميعية والتصاوير البيانية المعنية بدلاً عن بيانات تخص مكان وزمان المشتريات ومن هو الشخص القائم بتلك التعاملات.

عملياً، وفي حالة عدم التفاوض بهذا الشأن مسبقاً، فإنه قد لا يرغب مقدم الخدمات المالية بإعداد التقارير المحددة أو أن يعطوك معلومات محددة للغاية إذ أن ذلك يشكل جهداً إضافياً. الخيار الآخر في هذه الحالة، يتمثل بالطلب من مقدم الخدمات المالية **بعدم** موافاتك

بالمجموعة الكاملة من بيانات المدفوعات وإنما الاقتصار على قدر محدود من الحركات المالية وذلك لحماية خصوصية المستفيدين. ينبغي مطالبة مقدم الخدمات المالية بإزالة الأسماء وأرقام البطاقات لأي حركة مالية.

إذا كان الخيار الأوحد هو استلام بيانات الحركات المالية الكاملة وبشكلها الخام، من مقدم الخدمات المالية، فمن المستحسن الحد ممن له أن يستلم ويطلع على البيانات الكاملة وجعل هذا الشخص بمثابة «الحارس» ضمن فريقك. يقوم مقدم الخدمات المالية بإرسال بيانات المدفوعات إلى هذا الشخص حصراً. عندئذ يستطيع الحارس أن يستخلص فقط المعلومات اللازمة ليتسنى لبقية أعضاء فريق البرنامج معالجة هذه البيانات. عندها يستطيع الحارس حذف البيانات الكاملة، المستلمة من مقدم الخدمات المالية، بطريقة آمنة، وذلك لكي لا تستخدم سهواً لغرض آخر. توفر المعلومات التجميعية الملخصة مستوى أعلى في حماية البيانات وقد تكون وافية في العديد من الحالات.

مثال:

برنامج نقدي يصرف النقد باستخدام المحافظ النقدية في الهواتف المحمولة الخاصة بالمستفيدين. تود الجمعية الوطنية أن تعرف من هم وكلاء الصيرفة المتنقلين الذين تم استخدامهم في تحصيل النقد وذلك لتمكين الجمعية من إبلاغ جهات البيع في حالة وجود إشكالات في السيولة. عدم استطاعة مقدم الخدمات المالية الاقتصار على تقديم هذه المعلومات وإنما يرغب في إرسال قائمة الحركات المالية الكاملة مع جميع النشاطات المالية لكل فرد من المستفيدين وأماكن تحصيلهم للنقد. يقوم فريق برنامج العمل بإبلاغ مقدم الخدمات المالية بإرسالها حصراً إلى مدير المعلومات المتولي للبرنامج النقدي والذي بدوره يقوم باستخلاص البيانات اللازمة ليقوم فريق برنامج العمل بمعالجتها. يقوم مدير المعلومات بحذف الملف وذلك بعد استخلاصه حصراً لتلك البيانات التجميعية التي يحتاجها الفريق.

الحساب الإلكتروني للجمعية الوطنية

عندما يتم الصرف من خلال الحسابات الإلكترونية للجمعية الوطنية (أنظر الفصل الخاص بمقدمي الخدمات المالية)، قد لا يتوفر رابط مباشر بين الحركات المالية والمستفيدين الفعليين، وذلك لأن السيطرة على الحسابات الفرعية تتم من قبل الجمعية الوطنية. وعليه، فإن أمكانية ألاطلاع المباشر على الحركات المالية للمستفيدين، بحكم ملكيتك للحساب، قد يشكل تهديدا على الخصوصية. وكما تم تناوله، فإن بيانات المدفوعات الخاصة بالأفراد هي بيانات حساسة وقدر تعلق الأمر بالرقابة فإنه ليس من الضرورة، اعتياديًا، المعرفة بشؤون الأفراد من المستفيدين بل المعرفة بمجموعة منهم ككل.

ومرة أخرى أحدى الطرق لحماية خصوصية المستفيدين هي بترشيح شخص بمقام "بواب" حيث أنه الوحيد الذي يمتلك حق الوصول إلى كل المعاملات التي تجرى في المنصة. بتعيين شخص واحد فقط من الفريق للوصول إلى المنصة وتحويل البيانات الفردية إلى بيانات مجردة(تجريدية)، سيتم تقليل خطر حماية البيانات. في حال لم يكن من الممكن ترشيح حارس، ستكون مسؤولية جميع أعضاء الفريق الذين يمتلكون حق الوصول إلى المنصة والبيانات، احترام سرية وخصوصية البيانات وأيضاً ضمان أن معرفي الحسابات الثانوية غير مرتبطين بأشخاص معينين – هذه الخطوة حاسمة في جعل جميع أعضاء الفريق على دراية بمبادئ حماية البيانات.

حاول متابعة البرنامج بدون الحصول على بيانات شخصية من المستفيدين من مقدم خدمة التمويلFSP. متى ما وصلتك مثل هذه البيانات(الشخصية) يجب عليك أن تبلغ المستفيد وأن توضح له كيف تنوي حماية بيانات المستفيدين.

قرار المشروع 3: ماذا يمكن للتاجر إعطائي من بيانات المستفيدين في برنامج القسائم؟

الحصول على الحد الأدنى والضروري من البيانات وأمانها

إعادة صياغة مشروع القرار: ماذا يمكن للتاجر إعطائي من بيانات بهدف المتابعة بدون انتهاك لخصوصية المستفيدين؟

في البرامج المعتمدة على القسائم، يمكن استخدام بيانات المعاملات من التاجر للمتابعة والرصد. سيمتلك التاجر سجل لعدد القسائم التي صُرفت وتاريخ صرفها، وسيمتلك أيضاً سجل بالبضائع التي أُستبدلت بالقسائم. على أية حال، من المهم ضمان درجة عالية من حماية البيانات عند استخدام مثل هذه المعلومات. يكفي بشكل عام مراجعة البيانات المجمعة من الاستخدام العام للقسائم والسلع المشتراة. بهدف المتابعة، ليس من المهم معرفة استخدام مستفيد واحد من القسائم. بل المهم هو فهم السلوك العام للمستفيدين لتقييم مدى كفاءة البرنامج. لذلك يجب الابتعاد عن مراجعة البيانات المتعلقة بمتى وأين قام شخص واحد من المستفيدين بشراء سلعة معينة. يمكن إتمام

هذا بأن تطلب من التاجر جمع البيانات لك. إذا لم يكن هذا ممكناً فيمكن أن تطلب بيانات محددة بدون أي معرفات. عدا ذلك – كما في القسم السابق – رشح حارس ضمن فريقك يستقبل ويستخرج البيانات المطلوبة، ويمسح لائحة التعاملات مباشرة.

VIII. إرشادات عامة

ينظر هذا القسم في الإجراءات الرئيسية الممكن تطبيقها لحماية البيانات خلال البرنامج المالي.

اعتبارات حماية البيانات

تخزين البيانات

عند جمع البيانات الشخصية للمستفيدين، من المهم جداً إبقاءها بأمان وحمايتها. هذا يعني اتخاذ الإجراءات اللازمة لمنع اختراق البيانات(مثل ضياع البيانات، أو فقدان تصريح الدخول، ألخ...) (انظر في الأسفل للمساعدة في حالة اختراق البيانات).

الحلول التقنية لأمن المعلومات معقدة للغاية، وتتطلب في الغالب خبير بهذا المجال. لذلك يفضل تطوير منهجية محكمة بالتعاون مع إدارة تقنية المعلومات IT إذا أمكن. يمكن لهذه المنهجية أن تحدد تدفق البيانات، القنوات والواجهات لاستبدال البيانات، مستوى التشفير عند تخزين ونقل المعلومات، مع النسخ الاحتياطي لمنع فقدان البيانات، والتحكم في الوصول؛ للتأكد من أن المصرح لهم فقط يمكنهم استخدام البيانات، إلخ.

على أية حال، يجب مراعاة النقاط الآتية:

- للبيانات الرقمية، من المهم للغاية استخدام حلول وقواعد بيانات متينة قدر الإمكان. تجنب تخزين البيانات في مواقع التخزين المتوفرة للعامة مثل "Dropbox" و"Google". لاستخدام قواعد البيانات العديد من الميزات، لإنها توفر الحماية للبيانات، على سبيل المثال تشفير الأصل، ملفات محمية بكلمة مرور، والنسخ الاحتياطي، ألخ. يمكن لبرامج إدارة البيانات(مثل RedRose وLMMS) أن تُستخدم وتتفاعل مع برامج تجميع البيانات(مثل ODK أو Kobo) وآليات الدفع(مثل البنوك والنقد عبر الجوال) لتحويل الأموال. من المهم تقييم هذه الحلول لضمان حماية البيانات سواء في حالة الجمع (على سبيل المثال عند استخدام تطبيقات الهاتف لجمع البيانات مثل ODK / Kobo لرفع البيانات إلى الخادم) أو في حالة الراحة (عندما تكون البيانات مخزنة في السحابة). يجب تقييم الموقع المكاني لتخزين البيانات بالنسبة لقوانين الدولة (لأن بعض الدول تمنع أو تضع قيود لنقل البيانات خارج نظامها القضائي).
- خطر احتمالية فقدان أو سرقة البيانات عند تخزينها في وحدة USB أو اللاب توب تكون أكبر من تخزينها في قاعدة بيانات مناسبة. يجب تبني إجراءات حماية أكثر لتقليل هذه المخاطر. يجب حماية جهاز التخزين بمشفر للقرص الصلب (مثل Bitlocker من شركة مايكروسوفت). بالإضافة إلى ذلك، يمكنك إضافة طبقة حماية أخرى بتشفير أو وضع كلمة مرور للمستندات الموجودة في القرص الصلب. يجب أيضاً حماية أجهزة اللاب توب ووحدات USB باستخدام الأقفال والأدراج المقفلة عند عدم استخدامها.
- ضع كلمة سر قوية ومعقدة يصعب تخمينها. لفعل هذا استخدم حروف كبيرة وصغيرة، وأرقام، ورموز، وقم بتغيير كلمة السر من وقت لآخر. تجنب مشاركة الحسابات وكلمات المرور. إذا كان الحساب عام(أي يتم استخدامه وإدارته من قبل أكثر من شخص)، فمن المهم تقليص عدد الأشخاص(انظر في الأسفل – التحكم بالدخول).
- أما الملفات الورقية فلها احتمال أكبر لفقدانها أو الوصول لها بشكل غير مصرح. إذا كانت الملفات الورقية الخيار الوحيد، فيجب حفظها في مكان آمن ومقفل. مع أن استخدامها قد يحد من وصولها إلى أطراف ثالثة.

للمزيد من النصائح انظر إلى نشرة حماية البيانات من IFRC IM، لمعرفة ما يجب فعله وتجنبه وانظر أيضاً إلى سياسة أمن المعلومات لIFRC.

حفظ البيانات ومسحها

ما مصير بيانات المستفيدين الشخصية بعد انتهاء البرنامج؟ في العادة لا يتم الاحتفاظ بالبيانات لفترة لا محدودة. بمجرد عدم الحاجة للبيانات يجب مسحها، أو على الأقل يجب تجميعها أو إخفاء هويتها. إذا كانت البيانات مطلوبة لفترة مطولة (مثلاً في حالة التدقيق والمراجعة)، فيمكن أرشفة البيانات بطريقة آمنة وغير متصلة بشبكة الأنترنت.

فترات الاحتفاظ بالبيانات

يفضل أن تحدد المدة التي يجب الاحتفاظ بالبيانات فيها مسبقاً. بمجرد انتهاء فترة الاحتفاظ بالبيانات، يتم مسحها مباشرة. إلا إذا كانت هناك أسباب اضطرارية لبقاء البيانات فترة أطول، فيمكن ذلك لفترة محدودة. يمكن تسجيل فترة الاحتفاظ بالبيانات في قواعد البيانات نفسها بحيث يتم مسحها تلقائياً عند انتهاء المدة. لمعرفة المزيد حول هذه الإمكانيات، تواصل مع مختصي تقنية المعلومات في منظمتك. يمكن استخدام تنبيهات التقويم للتذكير بخصوص فترة الاحتفاظ بالبيانات، إذا لم يكن من الممكن عمل ذلك أوتوماتيكياً في قواعد البيانات. الهدف هو التفكير بنشاط في فترات منتظمة حول ما إذا كان سيتم الاحتفاظ بالبيانات التي لم تعد هناك حاجة إليها أو محوها.

يعتمد طول مدة الاحتفاظ بالبيانات على البرنامج نفسه، ولكن يمكن تحديده أيضاً بناءً على سياسات الخصوصية الخاصة بمؤسستك الخاصة. عند تصميم تدخل المساعدة النقدية، ينبغي مراعاة الفترات المناسبة للاحتفاظ بالبيانات حتى يمكن إبلاغها إلى الجهات المستفيدين. بعض الجوانب التي يجب مراعاتها هي:

- طول المشروع
- سرية البيانات
- حجم المراقبة المخطط لها
- احتمالية مشكلات المتابعة

أهداف أخرى

حتى إذا أغلق البرنامج وتم إجراء المراقبة، فقد يبدو من المفيد الاحتفاظ ببيانات معينة لأغراض أخرى. أولاً، يمكن استخدامهم لإنشاء **تقارير وإحصاءات** إضافية. إلا أنه ليس من الضروري عموماً إبقاء البيانات المتعلقة بهويات الأفراد (على سبيل المثال: الأسماء، بطاقات الهوية، الأرقام) لهذا الغرض. يكفي إنشاء مجموعة مركزة وإجمالية من البيانات. ثانيًا، خاصة بالنسبة للمناطق المعرضة لنفس المخاطر، من المحتمل أن تكون البيانات مفيدة في **الاستعداد العام للبرامج المماثلة المستقبلية** (على سبيل المثال، الأعاصير المتكررة أو الأعاصير). في هذه الحالات، قد يبدو من المعقول الاحتفاظ بالبيانات. غير أن البيانات تميل إلى أن يكون عمرها الافتراضي محدود. وبالنسبة للبرامج الجديدة، يلزم تحديثها والتحقق منها. يغادر الناس المنطقة أو ينتقلون إليها، أو تتغير ظروفهم المعيشية، أو يولد الأطفال، أو يموت أفراد الأسرة. ومن ثم، فإن الاحتفاظ بالبيانات لبرنامج جديد محتمل غالبًا ما يكون غير مفيد. إذا قررت الاحتفاظ بالبيانات لبرنامج مستقبلي، فمن المهم أيضًا التفكير فيما إذا كان الغرض الجديد متوافقًا مع الغرض الأصلي. قد تكون الأغراض الإنسانية متوافقة، ولكن إذا كان الغرض غير متوافق، فمن الضروري إبلاغ الجهات المستفيدة بنيتك في إعادة استخدام البيانات لغرض آخر وتحديد أساس قانوني جديد لهذه المعالجة الجديدة (راجع قسم الأساس القانوني في فصل التسجيل). ثالثًا، قد يتعين تخزين البيانات **لأغراض التدقيق**. إذا كان الأمر كذلك، فإن متطلبات التدقيق تحدد عادة فترات التخزين المطلوبة. إذا لم يكن الأمر كذلك، فيمكن غالبًا تحديد فترة تخزين معقولة من خلال النظر في الإطار الزمني و/ أو الغرض من التدقيق. يجب أرشفة البيانات المخزنة لأغراض التدقيق بشكل منفصل عن تدفق البيانات الأخرى.

بيانات غير المستفيدين

في عملية الاستهداف، تقوم بجمع البيانات الشخصية من الأشخاص الذين قد لا يستفيدون في النهاية من المساعدة لأنهم لا يستوفون فحص الأهلية (انظر فصل الاستهداف). وبالمثل، أثناء تسجيل المنتفع، ربما تكون قد جمعت بيانات من أشخاص يتضح في النهاية أنهم غير مؤهلين. يجب النظر بعناية فائقة في تخزين البيانات الشخصية لهؤلاء غير المستفيدين. نظرًا لأنهم لن يشاركوا في البرنامج، لم تعد هناك حاجة لبياناتهم بمجرد اكتمال التحقق من الأهلية. ومع ذلك، قد يكون من مصلحتكم بل ومن مصلحة غير المستفيدين الاحتفاظ بمعلوماتهم الشخصية لفترة معينة من الزمن. ويمكن أن يكون أحد الأسباب هو الحصول على دليل على القرارات إذا قام غير المستفيد برفع شكوى ضد الجمعية الوطنية لاستبعاده من البرنامج. في هذه الحالة، قد يكون من المفيد جدًا أن تكون قادرًا على معرفة كيف تم تحديد ذلك وما هي نقاط البيانات التي تم استخدامها في القرار. إذا أمكن، في مثل هذه الحالات، قم بتخزين المعلومات المعنية بشكل منفصل عن بقية المستفيدين المؤهلين الآخرين. الفكرة هي أن هذه البيانات لم تعد جزءًا من تدفق البيانات في البرنامج الجاري. ولكن، إذا ظهرت شكوى، فيمكن استعادتها.

صلاحية الدخول

يجب التعامل مع المعلومات التي يتم جمعها مباشرة من المستفيدين أو من مصادر أخرى (الحكومات، إلخ) بسرية تامة. ترتبط السرية ارتباطًا وثيقًا بمبادئ تقليل البيانات وبحكم الضرورة وأمن البيانات كما هو موضح أعلاه.

تشمل البرامج النقدية عادةً جهات معنية مختلفة: داخليًا (على سبيل المثال، البرنامج المباشر والأفرقة الميدانية، وخدمات الدعم مثل الزملاء من الشؤون المالية، واللوجستيات، وإدارة الرسائل الفورية، وتكنولوجيا المعلومات، والمديرين) والخارجيين (على سبيل المثال، مقدمي الخدمات المالية، والجهات المانحة، والحكومة، والمنظمات غير الحكومية الأخرى). لقد نظرنا بالفعل في التعامل مع البيانات الشخصية مع الجهات المعنية الخارجية (راجع الفصول الخاصة بمقدمي الخدمات المالية ومشاركة البيانات مع جهات خارجية). بالنسبة للجهات المعنية الداخلية، من المهم تحديد نوع الدخول ومستوى الدخول المطلوب فيما يتعلق ببيانات المستفيدين. بعض المنظمات تملك تصنيف للمعلومات. على سبيل المثال، تصنف سياسة أمن المعلومات للاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر بيانات المستفيدين على أنها سرية أو سرية للغاية حسب السياق؛ وهذا يتطلب أعلى مستوى من الحماية الأمنية بالإضافة إلى الدخول المحدود "على أساس الحاجة إلى المعرفة".

بعض الطرق لضمان التحكم المناسب في الدخول:

- استخدم اسم المستخدم وكلمة المرور للدخول إلى قاعدة البيانات أو منصة إدارة البيانات. أبلغ المستخدمين بعدم مشاركة اسم المستخدم وكلمة المرور الخاصة بهم مع الآخرين. أيضًا، تجنب إنشاء مستخدمين عامين حيث يمكن لعدة أشخاص تسجيل الدخول بصفتهم هذا المستخدم. يجب أن تكون نشاطات كل مستخدم قابلة للتدقيق والتتبع.
- استخدم التحكم المحدد في الوصول إلى المستند مما يعني منح المستخدمين أدوارًا محددة وكل دور يمنح الوصول إلى وظائف وبيانات معينة في النظام. يمكن أن يكون الدخول محدوداً حسب الضرورة (على سبيل المثال، الوصول إلى قائمة المستفيدين، أو القدرة على تنزيل قائمة المستفيدين، أو مجرد منح حق الوصول إلى البيانات المجمعة مثل لوحات المعلومات). يجب إلغاء تفعيل الدخول إذا كانت هناك مشكلة أمنية مع المستخدم.
- امتلك سجل دخول لتسجيل كل شخص يقوم بتسجيل الدخول والوصول إلى صفحات أو بيانات معينة، بالإضافة إلى سجل تنزيل لأولئك الذين يقومون بتنزيل البيانات مباشرة من النظام (مع ملاحظة أن هذا يعتبر أيضًا تجميعًا للبيانات الشخصية ومعالجتها ويجب التعامل معه بشكل مناسب).
- عند تنزيل البيانات في جدول بيانات Excel، أضف الحماية بكلمة مرور أو قم بتشفير الملف.
- في حالة عدم وجود قاعدة بيانات، يجب أن تكون الملفات محمية بكلمة مرور ويجب ألا يتمكن من الدخول إلى الملفات إلا الأفراد المصرح لهم. بالنسبة للملفات الورقية، يجب أن يتمتع الموظفون المعتمدون فقط بدخول مباشر ويجب الاحتفاظ بالملفات في حاوية مغلقة.

أمثلة:

يشمل البرنامج النقدي 10 موظفين ومتطوعين للتنفيذ. في حين أن 3 مسؤولين عن الاستهداف وتسجيل المستفيدين (الفريق 1)، فإن السبعة الآخرين مسؤولون فقط عن الاتصال بمقدمي الخدمات وتوزيع النقود (الفريق 2). لا يحتاج الفريق 2 إلى معرفة أوجه ضعف المستفيدين. يحتاجون فقط إلى معرفة البيانات الشخصية الضرورية مثل الجزء النقدي من المشروع (الأسماء، الحسابات المصرفية، اعرف عميلك). لذلك، ينشئ الفريق 1 لهم، قائمة بالمستفيدين باستخدام معلومات محدودة. تُخزن جميع المعلومات الأخرى في قاعدة بيانات محمية بكلمة مرور، ويكون الفريق 1 فقط لديه كلمة المرور هذه. علاوة على ذلك، هناك شخص واحد فقط لديه دور المسؤول ويمكنه الوصول بشكل كامل إلى قاعدة البيانات (الوصول للقراءة والكتابة)، بينما يمتلك عضوًا الفريق الآخران حق الوصول للقراءة فقط.

وفي نفس السيناريو، تكون طريقة التوزيع نقدية في مغلفات. ومن المتوقع أن يكون على الفريق الثاني أن يبرر اختياره للمستفيدين في يوم التوزيع. وإذا حدثت حالة من هذا القبيل، من الضروري أن يتمكن الفريق الثاني من الاطلاع على المعلومات الإضافية. ولذلك، يطلبون المعلومات الإضافية من الفريق الأول الذي يقدم المعلومات الإضافية المحدودة.

عملية الإرسال (مشاركة البيانات)

عند مشاركة البيانات، من المحتمل أن تزيد عملية الإرسال من خطر فقدان البيانات والوصول غير المسموح به. ولذلك، فإن التدابير الأمنية تلعب دوراً هاماً عند نقل البيانات الشخصية.

- وتُقسم البيانات بشكل مثالي باستخدام **أدوات مضمونة** مثل FTP الآمنة مع اسم المستخدم وكلمة السر والوصول المحدود لتحميل البيانات من قاعدة البيانات الآمنة أو منصة إدارة البيانات.

- وحيثما تكون الاتصالات المتعلقة بالمستفيدين في حاجة إلى إرسالها عبر **البريد الإلكتروني**، فمن الأهمية أن نتذكر ما يلي: (1) الحد من عدد المتلقين، (2) حماية الملحقات بكلمة سر (3) تشفير البريد الإلكتروني (عند الإمكان). وهذا يوفر بعض الحماية في حالة اختراق البريد الإلكتروني أو إرساله عن طريق الخطأ إلى عنوان خاطئ. ويقل خطر تعريض بيانات المستفيدين للأشخاص غير المصرح لهم عندما تُشفر الرسائل الإلكترونية والملحقات. إذا لم تتأكد من كيفية تشفير الملفات أو الرسائل الإلكترونية، يرجى الاتصال بزملائك في تكنولوجيا المعلومات. قد يبدو إرسال الرسائل الإلكترونية إلى القوائم البريدية بدلاً من إرسال الرسائل إلى الأفراد مناسباً ولكن يمكن أن يكون ذو إشكالية إذا كنت لا تعرف بالضبط من هو مدرج في القوائم البريدية. ويصح الشيء نفسه عند إرسال عناوين البريد الإلكتروني العامة، حيث يمكن أن يكون هناك أشخاص مختلفون يحملون كلمة السر أو يديرون حساب البريد الإلكتروني العام. توخ الحذر أيضًا عند إعادة توجيه رسائل البريد الإلكتروني أو عند إنشاء سلاسل البريد الإلكتروني من خلال جعل الأشخاص يردون على الرسائل. ومع زيادة أعداد المتلقين أو تغييرهم، احرص على ضمان الإذن للمتلقين الجدد أيضاً بالإبلاغ بالبيانات الشخصية للمستفيدين.

على سبيل المثال:

تُناقش حالة بعض المستفيدين المحتملين عن طريق البريد الإلكتروني مع قادة المجتمع المحلي لتقرير ما إذا كانوا مستحقين للحصول على البرنامج النقدي. ويمكن إرسال البريد الإلكتروني إلى زعيم المجتمع المحلي الذي يساعد في صنع القرار وإلى الزملاء المشاركين في الاستهداف. ومع ذلك، ينبغي تجنب إرسال البريد الإلكتروني إلى عنوان بريد إلكتروني عام مثل "cashteam@community.info@" "."

- احذر، إذا كنت تريد مشاركة الملفات التي تحتوي على بيانات شخصية عبر **تطبيقات المراسلة للجوال**، مثل WhatsApp. وما لم تكن واثقاً في أمن تطبيق المراسلة (على سبيل المثال، يُعتَبَر سيجنال على نطاق واسع أكثر أمناً من واتساب)، **فلا تستخدمه** لتبادل البيانات الشخصية أو غيرها من البيانات الحساسة (سواء من الموظفين أو المتطوعين أو المستفيدين).

معالجة انتهاكات البيانات

وعلى الرغم من جميع التدابير الأمنية، لا يوجد ضمان لمنع حدوث خرق للبيانات في جميع الحالات. *وكما هو محدد في بداية هذا التوجيه، فإن خرق البيانات يعني الوصول غير المسموح به إلى البيانات الشخصية أو تدميرها أو فقدانها أو تغييرها أو إفشائه.* وبمجرد حدوث خرق للبيانات، من المهم اتخاذ الخطوات الصحيحة لمعالجة عواقب الخرق. ويوصى بأن تعي أنت وموظفيك هذه الخطوات قبل حدوث أي خرق. بمجرد أن تعلم بحدوث خرق للبيانات، تأكد من:

- **تقديم تقرير دون أي تأخير** إلى مديركم أو مشرفكم وكذلك إلى منسق حماية البيانات أو الفريق القانوني أو شخص آخر مسؤول عن حماية البيانات في مجتمعكم الوطني. إذا كنت لا تعرف من هو المسؤول، أفصح عن مخاوفك إلى القيادة في منظمتك.

وينبغي عندئذ تنفيذ الخطوات التالية بالتعاون مع هؤلاء الخبراء:

- **التحقيق في مدى الإخلال وخرق المعلومات:** أي نوع من الخرق؟ أي نوع من البيانات؟ كم من البيانات؟ ما هي مدة الخرق؟ ما هو موضوع البيانات؟ لمن عُرضت المعلومات؟
- **(بالتوازي مع ذلك) اتخاذ تدابير الحد** (تبعاً لنوع الخرق، *مثلاً*، لخفض نظم تكنولوجيا المعلومات، واستعادة البيانات الاحتياطية، والاتصال بشخص غير مرخص له لإنهاء التعرض للبيانات، وإغلاق الثغرات، وإبلاغ الشركاء المعنيين، والمانحين المحتملين.
- **تقييم مستوى المخاطر بالنسبة لمواضيع البيانات وبذل جهود ممكنةً لإرشاد مواضيع البيانات إذا كانت المخاطر كبيرة** لأسباب تتعلق بالشفافية.
- **خذ بعين الاعتبار إبلاغ سلطات حماية البيانات في بلدك** وفقاً للقوانين الوطنية.
- **إعداد التقرير/الدروس المستفادة والقضاء على أوجه الضعف التنظيمية أو التقنية المحددة.**
- **تحسين خطة الاستجابة للحوادث التالية حسب** الحاجة استناداً إلى الخبرة المكتسبة.

إحاطة للموظفين والمتطوعين

والخطوة الأولى نحو الحماية الفعالة للبيانات هي الوعي. ولذلك، من المهم توعية موظفيكم ومتطوعيكم بالمبادئ الرئيسية لحماية البيانات وكيفية معالجتها في دورة برنامج المساعدات النقدية والقسائم. ويوصى بعقد دورات تدريبية منتظمة بشأن حماية البيانات، لا سيما تلك المنظمات الجديدة كجزء من انطلاقتها. ويمكن إعداد مواد تدريبية مسبقاً لانطلاقة المنظمات وأيضاً كنشاط تحفيزي للذين تم تدريبهم من قبل. وفي هذا التدريب، ينبغي إبراز أهمية حماية البيانات وشرح المبادئ الرئيسية. والأهم من ذلك، ما هي اعتبارات حماية البيانات التي ينبغي تناولها في إطار عمليات برنامج مساعدات النقد والقسائم ومسؤوليات الموظفين والمتطوعين وفقاً لأدوارهم. كما ينبغي أن يكون هناك وعي بكيفية التصدي لانتهاكات البيانات.

تحليل ورصد مخاطر حماية البيانات

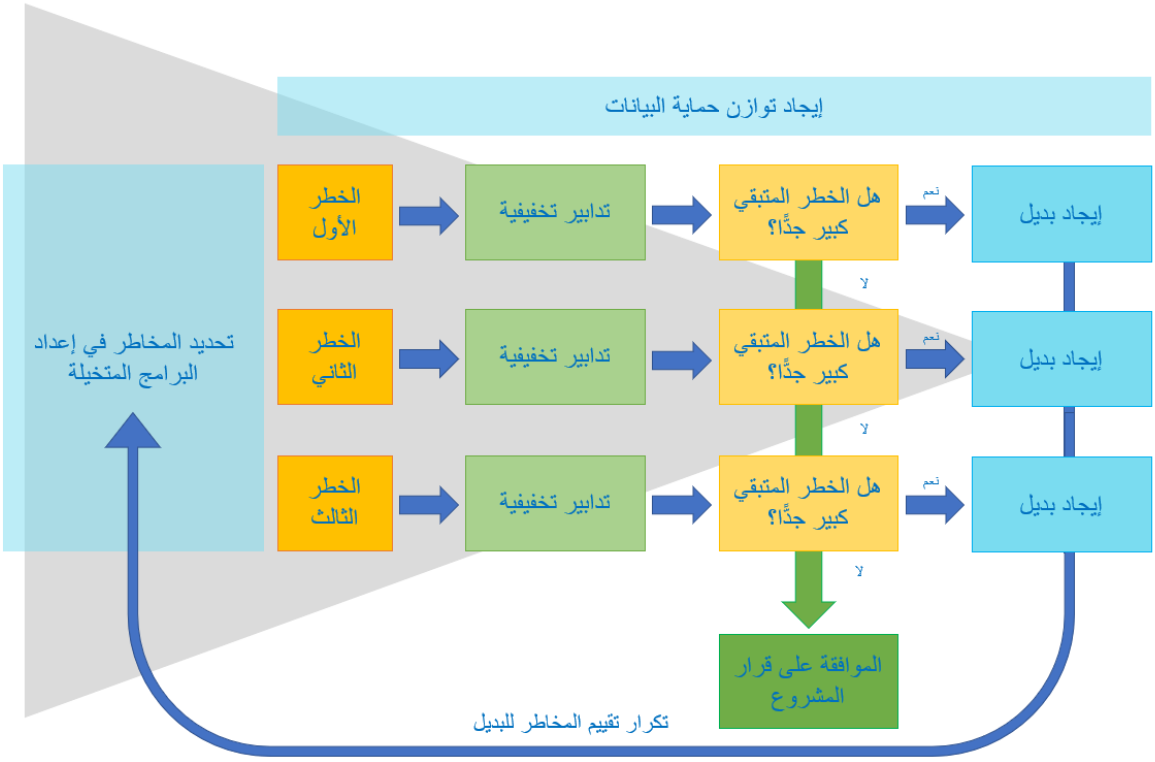
ولجعل حماية البيانات ضماناً حقيقياً لخصوصية المستفيدين في برامجكم، يوصى بشدة بأن تلاحظوا اعتبارات حماية البيانات التي تقومون بها. لماذا؟ لأنه يساعد على وضع نهج منظم ومتسق لإدارة المخاطر وإيجاد توازن جيد. كما أن توثيق المخاطر والقرارات المتخذة سيكون هاماً في حالة ما إذا كان من الضروري إجراء مراجعة أو تحقيق.

وهناك بعض الأدوات التي يمكن استخدامها في تحليل وتوثيق المخاطر المتصلة بحماية البيانات:

مصفوفة المخاطر وسجل المخاطر. وتغطي أدوات المساعدات النقدية في حالات الطوارئ.تحليل المخاطر في مجال الاستعداد والتأهب (الوحدة 1_1M والتحليل)، والتقييم (الوحدة 4_2M)، وتحليل الاستجابة (الوحدة 4_1_3M)). والمخاطر الإضافية الموصوفة لبرمجة النقدية مقابل العمل والقسائم أيضاً. ويمكن استخدام نفس مصفوفة وسجل المخاطر لضمان استعراض عناصر حماية البيانات

إلى جانب الأنواع الأخرى من المخاطر. وقد يلزم إنشاء فئة جديدة لحماية البيانات لتصنيف المخاطر على النحو المناسب. وسيكون من المهم تحليل هذه المخاطر ووضع تدابير للتخفيف منها. ومع تقدم البرنامج، ينبغي استعراض المخاطر وتحديثها حسب الحاجة.

تقييم تأثير حماية البيانات (DPIA).[14] يعد هذا التقييم أداة رسمية لتوثيق اعتبارات حماية البيانات بالنسبة للمخاطر المحددة فضلًا عن تدابير التخفيف المتوقعة. وقد يتطلب إعداده إجراء مشاورات خارجية وإشراك أصحاب المصلحة المعنيين مثل زملائكم القانونيين. وأداء تقييم تأثير حماية البيانات المتعمق ليس ضرورياً في جميع الحالات، ولا سيما عند تنفيذ برامج مساعدات النقد والقسائم المماثلة. وقد يكون من الضروري عند استخدام أساليب جديدة، استخدام التكنولوجيا عندما لا تكون الآثار على المستفيدين معروفة بعد. وسيكون من المفيد أيضا عندما يكون هناك مخاوف محتملة من أفراد المجتمع المحلي من حيث التعامل مع بياناتهم، لتحديد مكان المخاطر الفعلية وما إذا كان يمكن التخفيف منها.



شكل 4: موازنة المخاطر والإجراءات المتعلقة بحماية البيانات

ويهدف الشكل 4 إلى مساعدة عملية التفكير في تقييم مخاطر حماية البيانات. وينطوي ذلك على تحديد المخاطر والتدابير المخففة الممكنة، وتحديد مستوى المخاطر (على أساس الأثر والاحتمالات) والتقليل من الأخطار، وإيجاد بدائل لمراعاتها. على سبيل المثال:

إدراج مقدمي الخدمات المالية؟

>خطر 1: استخدام البيانات لأغراض أخرى إلى جانب ما تم الاتفاق عليه

> تدابير التخفيف: حظر في العقد

> هل تبقى مخاطرة كبيرة؟ نعم، لأن سمعة مقدمي الخدمات المالية ومصداقيتها مشكوك فيها

> البديل: مقدمي الخدمات المالية الأخرى، النقدية في الأظرف أو العينية

> تكرار تقييم المخاطر من أجل بديل

[14] انظر لمزيد من التفاصيل في دليل حماية البيانات في العمل الإنساني. كما، يمكن العثور على قالب DPIA (تقييمات تأثير حماية البيانات) في المقطع المرجعي من هذا التوجيه.

إذا كان التقييم الأولي للمخاطر يكشف أن إعداد البرنامج ينطوي على مخاطر عالية لحماية البيانات، فمن المستحسن إجراء التقييم باستخدام شكل تقييم تأثير حماية البيانات الرسمي. ويقع الالتزام بإجراء تقييم تأثير حماية البيانات الرسمي للأداء على عاتق المنظمة التي تقود البرنامج، في حالة الشراكة في التنفيذ.

وينبغي النظر في أداء نظام لتقييم تأثير حماية البيانات (وقد تكون هناك حاجة بموجب بعض قوانين حماية البيانات)، على سبيل المثال، في الحالات المذكورة أدناه. يرجى الملاحظة: وتخضع جميع طرق معالجة البيانات هذه بشدة لمبدأ تقليل البيانات إلى أدنى حد وضرورة. لا يمكن لتقييم تأثير حماية البيانات تبرير المعالجة غير الضرورية للبيانات.

- تُستخدم التكنولوجيا الجديدة لجمع البيانات الشخصية وإدارتها وتخزينها (التخزين السحابي، الموقع الجغرافي، وسائل التواصل الاجتماعي، إلخ). إن عدم معرفة كيفية عمل التقنيات الحديثة يمكن أن يزيد من خطر الوصول غير المصرح به (القرصنة) ويفتح الاحتمالات للمراقبة غير المصرح بها.
- قد يضطر الأفراد لاتخاذ القرارات الآلية أو التنميط. ويتدخل اتخاذ القرار الآلي بقوة في حماية البيانات، لأن القرارات تتخذ خارج نطاق سيطرة الفرد ودون إمكانية أن يتتبع الفرد القرار ويناقشه. التنميط هو إشكالية لأن إنشاء ملف تعريف للأشخاص هو مثل وضعها في فئات معينة دون تفاعل حقيقي مسبق مع الفرد.
- قد يتم نقل البيانات الشخصية إلى طرف ثالث (أو بلد) دون معايير حماية البيانات المماثلة. كما ذُكر، قد يؤدي مشاركة البيانات إلى فقدان التحكم في كيفية استخدام هذه البيانات. وينبغي أن يتم ذلك فقط عندما يكون لدى الطرف الآخر معيار حماية البيانات الكافي. وإذا لم يكن الأمر كذلك ويجب تبادل البيانات على أي حال، فمن المهم إجراء تقييم شامل لما إذا كان ذلك يشكل خطرًا كبيرًا على المستفيدين (فئة البيانات، ومعيار الحماية، وما إلى ذلك.)
- ويمكن معالجة البيانات الحساسة، مثل البيانات المتعلقة بالحالة الصحية أو التوجه الديني أو القياسات الحيوية على نطاق واسع (عدد الأشخاص، وتنوع البيانات، ومدة المعالجة، والنطاق الجغرافي، وما إلى ذلك). هذه البيانات حساسة للغاية لأنها تتعلق بجوانب شخصية وخاصة جدا من حياة شخص ما. وبالإضافة إلى ذلك، فإن هذا النوع من المعلومات في الأيدي الخطأ يمكن أن يكون ضارا جدا للمستفيدين.
- وقد تكون المراقبة الجماعية جزءا من البرنامج. وتتعارض المراقبة الجماعية بشدة مع حقوق جميع الأشخاص المعنيين، لأنها جزء هام من الخصوصية التي يجب أن لا تخضع لرقابة مستمرة من الآخرين أو من النظم الآلية.
- وقد تتوحد البيانات الواردة من مصادر مختلفة والربط بينها. الجمع بين مجموعات البيانات المختلفة على فرد واحد يزيد من المخاطر على خصوصية الفرد.

وبصرف النظر عن الشكل، ينبغي إجراء تقييم المخاطر قبل بدء البرنامج، إلى جانب التقييم العام للمخاطر بالنسبة للبرنامج على النحو المبين في مجموعة أدوات المساعدات النقدية في حالات الطوارئ.

إذا كانت هناك أسئلة ومخاوف تتعلق بحماية البيانات، فلا تتردد في التواصل مع مديرك و/أو فريقك القانوني. يمكنك أيضا إرسال الاستعلامات إلى Cash Hub، وهو مورد واسع الحركة لمساعدات النقد والقسائم. ويدعم مركز النقد الممارسين النقديين ويقدم مواد تشمل الدروس المستفادة من الجمعيات الوطنية الأخرى وربما تكون قد نظرت في أسئلة مماثلة من شركاء آخرين في الحركة في الماضي.

المشاركة المجتمعية والمساءلة

وكما نوقش في جميع الفصول، فإن إعلام المستفيدين ووجود مكتب للمساعدة وآلية للتغذية المرتدة هما جانبان هامان من جوانب تنفيذ حماية البيانات. عندما يتصل فريق المشاركة المجتمعية والمساءلة المستقل بالمستفيد، من المهم أن يكونوا على علم باعتبارات حماية البيانات وضمان أن يكون لديهم معلومات لمعالجة الأسئلة المتعلقة بحماية البيانات أو معرفة كيفية إحالة تلك الأسئلة إلى شخص يمكنه الإجابة عليها.

IX. مراجع

السياسات والتوجيهات

- دليل واحد عن حماية البيانات في العمل الإنساني من قبل اللجنة الدولية ومركز بروكسل للخصوصية
- سياسة الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر بشأن حماية البيانات
- قواعد اللجنة الدولية للصليب الأحمر بشأن حماية البيانات
- سياسة اللجنة الدولية للصليب الأحمر بشأن معالجة البيانات البايومترية
- سياسة الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر لأمن المعلومات
- نشرة حماية بيانات الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر

القوالب والمواد المساعدة

وينبغي للجمعيات الوطنية أن تضع المواد التالية في سياقها الصحيح: لتلبية الاحتياجات التي تنفرد بها؛ وعلى وجه الخصوص، الالتزام بقوانين وسياسات حماية البيانات الوطنية التي قد تكون أكثر صرامة من معيار حماية البيانات المطبق عند إعداد هذه الوثائق.

- قالب عقد معياري لموفر الخدمة المالية (مسودة عمل)
- استبيان مقدم الخدمة المالية قبل التعاقد/نموذج العناية الواجبة (مسودة العمل)
- قالب تقييم تأثير حماية البيانات (مسودة العمل)
- نموذج عينات الإشعار بالخصوصية (مسودة العمل)