المبدأ: التعامل مع الخصوصية والأمن

مقدمة

تتضمن معالجة الخصوصية والأمن في التطوير الرقمي، دراسة متأنية للبيانات التي يتم جمعها وكيفية الحصول عليها واستخدامها وتخزينها ومشاركتها. يجب أن تتخذ المنظمات تدابير لتقليل عملية جمع المعلومات السرية وهويات الأفراد الممثلة في مجموعات البيانات إلى أدنى حد ممكن للحد من الوصول والتلاعب غير المصرح به من قبل أي أطراف أخرى. تشمل الممارسات المسؤولة للمؤسسات التي تقوم بجمع واستخدام البيانات الفردية، مراعاة حساسية البيانات التي يتم جمعها، والشفافية حول كيفية جمع البيانات واستخدامها، مما يقلل من كمية المعلومات الشخصية الحساسة القابلة للتعريف، وإنشاء وتنفيذ سياسات أمنية تحمي البيانات وتدعم خصوصية الأفراد وكرامتهم، بالإضافة الى خلق سياسة واضحة لإدارة البيانات ما بعد إنتهاء المشروع.

المبادئ الأساسية

- **قم بتحديد ملكية البيانات والسيادة عليها قبل القيام بجمع أي بيانات.** حدد القوانين واللوائح المحلية لحماية البيانات التي يجب اتباعها، ومن الذي يتعين عليه أن يقرر ما يجب فعله بالبيانات، ومن يُسمح له بالوصول إلى البيانات أو استخدامها، وأين يمكن أو يجب تخزين البيانات.
- **حافظ على اهتمامات المستخدمين والأفراد الذين يتم جمع بياناتهم واجعلها في مقدمة خططك للحفاظ على خصوصية المستخدم وضمان أمن البيانات والتطبيق الأخلاقي.** يعتبر ذلك مهم بشكل خاص عندما يعمل المنفذون مع المجتمعات الضعيفة أو المهمشة التي قد لا يكون لها رأي في كيفية جمع بياناتهم أو استخدامها أو مشاركتها.
- **قم بإجراء تحليل لمخاطر منافع البيانات الجاري معالجتها،** والتي تحدد من المستفيد ومن هو المعرض للخطر. قد تحتاج هذه العملية إلى تكرارها طوال فترة حياة المشروع حيثما كان هناك حاجة إلى بيانات جديدة أو تحديد مخاطر جديدة أو النظر في شركاء جدد لتبادل البيانات.
- **قم بتقييم مخاطر** الوصول غير المصرح به أو تسرب أي بيانات مخزنة لديك. ضع في اعتبارك التأثير الذي قد تحدثه هذه البيانات على الأفراد إذا تم الوصول إليها أو نشرها بشكل ضار بالإضافة الى مخاطر دمج البيانات مع مجموعات بيانات أخرى.
- **تفهم أن المخاطر متعلقة بالسياق بشكل كبير،** ليس فقط للبلدان ولكن أيضًا للمجتمعات والسكان وفترات زمنية محددة. إذا كنت تعمل مع المجتمعات الضعيفة أو المهمشة، فما هي المجموعات التي قد يكون لديها الدافع للحصول على بياناتك؟ وما مدى قدرتها على ذلك؟ وهل تعد المعلومات والضوابط المتعلقة بالوصول إلى البيانات كافية؟

دليل دورة حياة المشروع

لقد تم استخلاص التوصياتيتم الحصول على التوصيات والنصائح والموارد التالية من مجتمع التطوير الرقمي لإعطائك خيارات لتطبيق هذا المبدأ خلال كل مرحلة من دورة حياة المشروع. لا يُقصد بهذا التوجيه أن يكون شاملاً، ولكنه يقترح بعض الإجراءات التي يمكنك اتخاذها لتطبيق هذا المبدأ في عملك. إذا كانت لديك نصائح أو موارد أو تعليقات أخرى لإضافتها، فيرجى مشاركتها على صفحة المنتدى.
https://forum.digitalprinciples.org

المبدأ: التعامل مع الخصوصية والأمن

- **قلل من جمع معلومات التعريف الشخصية.** ضع في اعتبارك مدى أهمية المعلومات الشخصية لنجاح المشروع، وما هي عواقب ذلك؟ خاصة إذا تعرضت هذه البيانات للمشاركة مع أطراف ثالثة - خاصة عند الشراكة مع المستخدمين من الفئات السكانية الضعيفة، مثل مجموعات الأقليات والمعوقين والنساء والأطفال. قم بتضمين تقييم للمخاطر الخاصة بجمع المعلومات الشخصية.
- **قم بفهرسة وتعقب أي معلومات شخصية أو حساسة تم جمعها خلال المشروع:** قم بوضع خطة للإزالة في منتصف وما بعد المشروع أو لتخزين آمن للبيانات الحساسة دون اتصال بالإنترنت، بما في ذلك مراجعة محركات الأقراص الثابتة وتخزين الملفات السحابية ومحركات أقراص (Flash Desk) وصناديق البريد الإلكترونية وغيرها من المصادر الشائعة لتسرب البيانات.
- **كن شفافاً** مع الأفراد الذين يتم جمع بياناتهم عن طريق شرح كيفية استخدام مبادرتك للبيانات وحماية بياناتهم.
- **قم بالحصول على موافقة موثقة** قبل البدء بعملية جمع البيانات. من المهم التأكد من أن المشاركين يفهمون سبب جمع بياناتهم، وكيفية استخدام البيانات ومشاركتها، وكيف يمكن للمشاركين الوصول إلى البيانات التي تم جمعها أو تغييرها ومنحهم خيار رفض المشاركة. يجب إطلاع المشاركين على المخاطر المتعلقة بمشاركة بياناتهم وفهمها تمامًا. كما يجب كتابة نماذج الموافقة باللغة المحلية وفهمها بسهولة من قبل الأفراد الذين يتم جمع بياناتهم.
- **قم بحماية البيانات** من خلال اعتماد أفضل الممارسات لتأمين وتقييد عملية الوصول إلى البيانات. تتضمن أمثلة أفضل الممارسات تشفير الملفات، واستخدام المصادقة الثنائية، وتقييد أذونات الدخول، وتخزين البيانات على خوادم آمنة أو من خلال خدمات التخزين السحابية الآمنة، وتنفيذ سياسات وإجراءات الأمن التنظيمية، بما في ذلك اتفاقيات مشاركة البيانات مع جميع شركاء تبادل البيانات.

يعد دعم هذه المبادئ أمرًا ضروريًا لضمان التنفيذ الأخلاقي لمبادرات التطوير الرقمي وتجنب النتائج السلبية التي قد تنجم عن انتهاكات أمن البيانات. يحمي اتباع ممارسات خصوصية البيانات وحماية الأمن مصالح المجتمعات، مع تعزيز الثقة بين المستخدمين النهائيين وممارسي التنمية الرقمية. يجب الحفاظ على سرية وأمن البيانات الشخصية بهدف الحفاظ على كرامة وأمن الأفراد المستخدمين للأداة.

«تذكر أن التدابير الأمنية والتقنية يجب ان تكون قوية تماماً مثل المستخدمين للتكنولوجيا. قم بتصميم الأمن الذي يمكن استخدامه في السياقات التي تستخدم فيها التكنولوجيا.»

CLAYTON SIMS
DIMAGI

حلّل وخطّط

في هذه المرحلة، فكر استراتيجياً في البيانات التي سيتم جمعها وكيف سيتم استخدامها خلال دورة حياة المشروع. قم بتحديد كيفية الحفاظ على سرية المعلومات الحساسة خلال كل مرحلة، مع الموازنة بين مخاطر البيانات التي قد يتم اختراقها مقابل ضرورة جمع البيانات التي تحتاجها.

- **حدد أي من البيانات تعتبر مهمة لنجاح المبادرة، واعمل على تحقيق التوازن بين جمع البيانات الحساسة الأساسية مع الحفاظ على مصالح الأفراد.** يجب أن تدرك أن عملية جمع البيانات قد يُعرض بعض المجموعات السكانية للخطر. قم بجمع الحد الأدنى من المعلومات الشخصية القابلة للتعريف والبيانات الحساسة؛ تأكد من الحصول على موافقة موثقة باستخدام النماذج واللغة المفهومة للأفراد الذين يتم جمع بياناتهم. بالإضافة الى النظر فيما إذا كان يمكن دمج مجموعات البيانات المجهولة لتحديد مستخدمين محددين وربط البيانات السرية المجهولة بهم.
- **قم بإجراء تقييم للمخاطر** لتحديد التهديدات الداخلية والخارجية التي قد تتعرض لها بياناتك، وكذلك نقاط ضعف النظام. قم بإعطاء الأولوية للتهديدات أو نقاط الضعف، مع مراعاة الضرر المحتمل وعدد المستخدمين المتأثرين بذلك، وقابلية الاستغلال ومخاطر السمعة. قم بوضع خطة لإدارة المخاطر تحدد فيها الإجراءات المضادة التي سوف تتخذها لمواجهة التهديدات ذات الأولوية العالية.
- **عليك النظر في تداعيات الاستدامة والتوسع** عند تحديد البيانات التي ستجمعها. قد تحتاج إلى جمع مزيد من المعلومات لدعم عملية النشر على نطاق واسع.
- **عليك فهم القوانين والانظمة المحلية المتعلقة بخصوصية البيانات وأمنها، بما في ذلك القوانين والأنظمة المؤسسية.** تحدث مع المسؤولين الحكوميين والقادة المحليين ومنظمي البيانات (مثل المنظمات متعددة الجنسيات ومسؤولي المستشفيات) والمستخدمين لمبادرتك. بالإضافة الى فهم العواقب المترتبة على عدم الامتثال مثل الغرامات أو العقوبات، وكذلك أي تأثير سلبي سيحدثه عدم الامتثال على سمعة مؤسستك وعلى نجاح المبادرة.
- **قم بوضع خطة لقدرة الرقابة.** قم بتحديد المسؤولية عن الأمن وإدارة المخاطر لأفراد محددين، وإجراء دورات التوعية الأمنية والتدريب لمستخدمي البيانات. عليك تحديد وتأمين تمويل مستمر للتدابير الأمنية والرقابة.

صمّم وطوّر

يجب إنشاء خطط لإدارة البيانات وأمنها واختبارها وإضفاء الطابع الرسمي عليها خلال هذه المرحلة. قد تقوم أيضًا بجمع البيانات لإعلام وتصميم وتطوير الأدوات الرقمية المستخدمة في البرنامج.

- **قم بإنشاء خطة لإدارة البيانات** قبل البدء بعملية جمع البيانات. توضح خطة إدارة البيانات ما ستفعله بالبيانات أثناء وبعد مبادرتك لضمان أن تكون البيانات قابلة للوصول اليها وبشكل آمن. حدد إجابات الأسئلة التالية في خطتك:
  - **جمع البيانات:** ما هو حجم البيانات التي سيتم جمعها؟ وعلى أي فترة سيتم جمع البيانات؟ ومن المسؤول عن جمع البيانات وإدارتها وأمانها؟

حلّل وخطّط

النصائح والمصادر والمراجع

نصيحة: اتبع أفضل الممارسات لجمع وإدارة البيانات الخاصة والمعلومات الحساسة:

- الحصول على موافقة موثقة من مالكي البيانات بشأن العمليات المستخدمة للوصول إلى البيانات الشخصية واستخدامها ومشاركتها.
- كن شفافاً مع الأفراد الذين يتم جمع معلوماتهم حول كيفية استخدامك لهذه المعلومات.
- قم بتحديد آليات للأفراد للوصول إلى معلومات حول كيفية جمع واستخدام بياناتهم الشخصية.
- قم بجمع البيانات الشخصية للاستخدام المحدد والعادل والمبرر فقط.
- عليك تقليل جمع البيانات وقصر تدوين البيانات على التفاصيل الأساسية.
- عليك فرض المعايير واتباع أفضل الممارسات للوصول إلى البيانات والتحديثات والإدارة.

RESOURCE: Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) https://SAFETAG.org

RESOURCE: The OECD Privacy Framework, Organisation for Economic Co-operation and Development https://digitalprinciples.org/wp-content/uploads/2015/12/oecd_privacy_framework.pdf

RESOURCE: European Union General Data Protection Regulation (EU GDPR) https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

RESOURCE: African Union Convention on Cyber Security and Personal Data Protection, African Union https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

RESOURCE: The Hand-Book of the Modern Development Specialist, Responsible Data Forum https://responsibledata.io/resources/handbook/

المبدأ: التعامل مع الخصوصية والأمن

- **التحقق من صحة ودقة البيانات:** هل تعتبر إزالة معلومات التعريف الشخصية جزءًا من عملية تنقيح البيانات، خاصةً البيانات النوعية؟
- **التنظيم والتخزين:** كيف تقوم بتوثيق وحفظ بياناتك لتكون مفهومة ويمكن الوصول إليها من قبل الآخرين؟ وما هي تنسيقات الملفات واتفاقيات التسمية التي تستخدمها؟ وما هي إجراءات التخزين الخاصة بك لضمان أمن البيانات؟
- **الوصول:** من لديه حقوق الوصول للبيانات؟ وكيف سيتم مشاركة البيانات؟ وكيف ستحمي البيانات الشخصية؟ وهل سيُسمح بإعادة استخدامها؟
- **الأرشفة:** كم من الوقت سيتم تخزين البيانات وحفظها؟ وكيف سيتم التخلص منها إذا لم تعد هناك حاجة لها؟ وكيف سيتم جعل البيانات مجهولة؟ هل يوجد مستودع مفتوح المصدر متاح لتخزين البيانات أم سيتم نقل البيانات إلى مؤسسة أخرى؟

قم بمواءمة خطتك مع سياسات الخصوصية والأمن وإدارة البيانات المسؤولة ومعايير مجتمع المصادر المفتوحة، إذا كان ذلك مناسبًا. شارك خطتك مع الشركاء والمستخدمين المستهدفين ومجتمع التطوير الرقمي الأوسع لتعزيز الشفافية والمساءلة والثقة. تأكد من أن الخطة مفهومة ومقبولة من قبل أصحاب المصلحة المختلفين.

- **حدد أعضاء الفريق الذين سيكونون مسؤولين عن إدارة البيانات والأمن طوال دورة حياة المشروع.** تشمل المسؤوليات إجراء التغييرات على خطة إدارة البيانات عندما تتغير البيئة الخارجية، وإجراء تحليل للمخاطر، ومراقبة البيانات للتأكد من أنها آمنة والاستجابة للانتهاكات الأمنية، وكذلك تدريب الأفراد الذين سيتولون ملكية البيانات، إذا كانت هناك نية لنقل المبادرة وتبنيها من قبل جهة أخرى.
- **قم بإجراء مراجعة منتظمة لوظائف النظام التي تجمع البيانات تلقائيًا.** أثناء التطوير، يمكن إضافة وظائف جديدة لجمع البيانات داخل النظام. هل يمكن أن تبرر المبادرة الحاجة إلى جمع تلك البيانات؟ وهل هناك سياسات واضحة حول كيفية جمع البيانات وتخزينها واستخدامها والتخلص منها؟
- **قم بتطوير الأداة الرقمية للالتزام بالمعلومات الحالية ومعايير الأمن الملموس لحماية المعلومات الشخصية.** على سبيل المثال، تأكد من أن النظام الأساسي الذي تستخدمه مبادرتك يمكنه إدارة وصول المستخدم وأذوناته لعرض البيانات أو استخدامها.

أنشر ونفّذ

خلال هذه المرحلة، ضع خطة لإدارة البيانات في موضع التنفيذ. بناءً على متطلبات المبادرة، قد تقوم أيضًا بجمع معلومات شخصية. قم بالاطلاع المنتظم بالبيانات التي تجمعها، وكيف يتم استخدام البيانات، وكيف يتم الحفاظ عليها بشكل آمن ومن يستخدم هذه البيانات.

- **عليك التحكم في الوصول إلى البيانات للحفاظ على النزاهة والسرية.** قم بإنشاء مجموعات الوصول مع أذونات محددة حسب أدوار المستخدمين. قم بوضع أدنى حد ممكن من الأذونات لمعظم الأفراد وبشكل افتراضي، وتمكين المزيد من الأذونات مثل الوصول للقراءة والكتابة فقط للمستخدمين الأساسيين. بالاضافة الى إعداد متطلبات كلمة المرور الفردية لجميع المستخدمين، وتفعيل استخدام المصادقة الثنائية للوصول الى البيانات. حيث تعتبر مصادقة العامل الواحد هي

صمّم وطوّر

المصادر والمراجع

RESOURCE: Data Management Plan Tool, Stanford Libraries https://library.stanford.edu/research/data-management-services/data-management-plans/dmptool

RESOURCE: Data Management, Massachusetts Institute of Technology Libraries https://libraries.mit.edu/data-management/plan/write/

RESOURCE: The Hand-Book of the Modern Development Specialist: Designing a Project, Responsible Data Forum https://responsibledata.io/resources/handbook/chapters/chapter-01-designing-a-project.html

RESOURCE: Beyond Data Literacy: Reinventing Community Engagement and Empowerment in the Age of Data, Data-Pop Alliance https://datapopalliance.org/item/beyond-data-literacy-reinventing-community-engagement-and-empowerment-in-the-age-of-data/

RESOURCE: Data Innovation Risk Assessment Tool, UN Global Pulse. https://unglobalpulse.org/sites/default/files/Privacy%20Assessment%20Tool%20.pdf

RESOURCE: Girl Safeguarding Policy: Digital Privacy, Security, & Safety Principles & Guidelines, Girl Effect https://www.ictworks.org/wp-content/uploads/2016/05/GE-Girl-Digital-Privacy-Security-Safety-v-May-2016.pdf

RESOURCE: Responsible Data Management, Oxfam https://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management

RESOURCE: Improving Data Privacy & Data Security in ICT4D: Meeting Report, UN Global Pulse https://www.unglobalpulse.org/blog/improving-data-privacy-data-security-ict4d-meeting-report

القيام بإدخال اسم المستخدم وكلمة مرور واحدة لتسجيل الدخول إلى الحساب. في حين ان المصادقة الثنائية، تمر بخطوة إضافية بعد إدخال كلمة المرور، مثل الحصول على رمز التحقق الذي يتم إرساله إلى رقم الهاتف المرتبط بالحساب عبر الرسائل القصيرة ثم إدخال الرمز للوصول إلى الحساب.

- **قم بتنفيذ التدابير المضادة للمخاطر ذات الأولوية ونقاط الضعف.** عليك الاستمرار في إجراء تحليلات منتظمة للمخاطر ومراجعات الأمن لتحديد نقاط الضعف الناشئة. قم بالرد فورًا على أي انتهاكات أمنية للتأكد من تخفيف الآثار السلبية بسرعة وسهولة، وإبلاغ الأفراد الذين تم انتهاك بياناتهم.
- **في حالة إغلاق المشروع، قم بتنفيذ خطة إما لحذف البيانات أو نقل البيانات إلى تخزين طويل الأجل.** قم بحذف أي سجلات تعتبر حساسة أو لم تعد مطلوبة للمبادرات الاخرى ولا تخدم أغراض التقييم في المستقبل. قم بإبلاغ أصحاب المصلحة المعنيين بكيفية إدارة البيانات أو إتلافها.
- **في حالة توسيع نطاق المبادرة أو نقلها، قم بالعمل مع أعضاء المبادرة أو المنظمات الجديدة لضمان الفهم والالتزام بخطة إدارة البيانات التي تم جمعها.** حدد أي فجوات في الأمن قد تنشأ عن عملية التوسع أو النقل. العمل مع الشركاء لمعالجة الثغرات وإجراء التحديثات اللازمة لخطة إدارة البيانات.

الشمولية والتقاطع: راقب وقيّم

استمر في متابعة خطة إدارة البيانات الخاصة بك، وقم بإجراء التحديثات حسب الحاجة استنادًا إلى نتائج المراقبة والتقييم.

- **ضع خطة لجمع البيانات بناءً على خطة الرصد والتقييم الخاصة بك،** مع تضمين الاعتبارات في خطة إدارة البيانات. تأكد من أن الموظفين مدربون تدريباً كاملاً على تنفيذ الخطة وأن جميع جامعي البيانات مدربون على أخلاقيات البحث. يقدم FHI٣٦٠ منهجًا تدريبيًا مجانيًا لأخلاقيات البحث لأخصائيين التنمية الدولية.
- **اتبع مكونات تنظيم البيانات والتخزين والوصول إلى خطة إدارة البيانات الخاصة بك. خلال جمع بياناتك،** تأكد من تخزينها بشكل آمن مع استمرار الوصول إليها. عليك النظر فيما يلي:
  - ما هو التسلسل الهرمي والتنظيمي لنظام الملفات؟
  - أين ستتواجد البيانات التعريفية لنظام الملفات، بما في ذلك خطة إدارة البيانات؟
  - ما هو نظام تسمية الملفات الذي ستستخدمه؟
  - كم عدد نسخ الملفات التي سيتم تخزينها في قاعدة البيانات الإلكترونية؟
  - هل سيتم استخدام أي من تقنيات الشبكات الخاصة بالمؤسسة لتخزين الملفات على سبيل المثال، تخزين مشترك أو تخزين سحابي؟
  - كيف سيتم أرشفة البيانات؟
  - ما التنسيقات مثل Microsoft Word و PDF التي سيتم حفظ البيانات المؤرشفة بها؟
  - كيف سيتم حماية البيانات المؤرشفة (على سبيل المثال، قاعدة البيانات المقفلة)؟
  - كم المساحة اللازمة لتخزين الملفات والتي ستكون ضرورية؟ هل هي متوفرة أم ستحتاج إلى شراء؟

أنشر ونفّذ

النصائح والمصادر والمراجع

نصيحة: استخدم قائمة للتحقق من حماية البيانات للتأكد من أن بياناتك آمنة. يمكنك أيضًا استخدام قائمة المراجعة هذه لوضع مؤشرات لرصد وتقييم أمن البيانات والخصوصية.

- هل كلمات مرور أجهزة الكمبيوتر محمية باستخدام كلمات مرور قوية؟
- هل تم تخصيص أرقام هوية مجهولة لجميع المشاركين في الدراسة؟
- هل تم تدريب جميع الموظفين على السرية والخصوصية؟
- هل جميع ملفات النسخ الاحتياطي آمنة؟
- تحت أي ظرف من الظروف سيتم تبادل البيانات ومع من؟ كيف سيتم مشاركة البيانات بطريقة آمنة؟
- هل يتم مراجعة وتحديث الإجراءات الأمنية بانتظام؟
- لا تحتفظ بالبيانات الموجودة على محركات أقراص Flash Deskأو غيرها من الأجهزة الخارجية التي يمكن فقدانها أو سرقتها بسهولة.
- لا تستخدم البريد الإلكتروني لإرسال معلومات تعريف عن المشارك.

RESOURCE: Data Protection, Privacy and Security for Humanitarian & Development Programs, World Vision International https://www.wvi.org/health/publication/data-protection-privacy-and-security-humanitarian-development-programs

RESOURCE: How to Develop and Implement Responsible Data Policies, MERL Tech http://merltech.org/how-to-develop-and-implement-responsible-data-policies/

RESOURCE: The Hand-Book of the Modern Development Specialist: Getting Data, Responsible Data Forum https://responsibledata.io/resources/handbook/chapters/chapter-02a-getting-data.html

المبدأ: التعامل مع الخصوصية والأمن

- **انتبه لمخاطر الخصوصية واجعل البيانات مجهولة المصدر لإزالة معلومات التعريف الشخصية.** استخدم رموز الهوية طوال عملية جمع البيانات وإدخالها حتى يمكن تتبع الردود دون انتهاك السرية. ويعتبر ذلك مهم بشكل خاص للسكان المعرضين للخطر أو المهمشين. كن على دراية بأن دمج مجموعات البيانات يمكن أن يعيد تعريف الأفراد.
- **قم بالنظر في القضايا الأخلاقية على نطاق أوسع.**
- **عليك القيام برصد المؤشرات المتعلقة بأمن البيانات والخصوصية.** توفر قائمة التحقق من أمن البيانات (في النصائح والموارد في قسم انشر ونفّذ) عدة مؤشرات محتملة.

الشمولية والتقاطع:
راقب وقيّم

النصائح والمصادر والمراجع

نصيحة: يعتمد التنظيم السليم لاستبيانات الاستقصاء وغيرها على الاستخدام المتسق لرموز التعريف خلال عمليات جمع البيانات وإدخالها. تساعد رموز التعريف في ضمان إمكانية تتبع جميع المعلومات وربطها بغض النظر عن المصدر.

RESOURCE: The Hand-Book of the Modern Development Specialist: Sharing Data, Responsible Data Forum https://responsibledata.io/resources/handbook/chapters/chapter-02c-sharing-data.html

RESOURCE: Ethical Guidelines for Educational Research, British Educational Research Association (BERA) https://www.bera.ac.uk/researchers-resources/publications/ethical-guidelines-for-educational-research-2011

RESOURCE: Research Ethics Training Curriculum, FHI360 https://www.fhi360.org/sites/all/libraries/webpages/fhi-retc2/RETCTraditional/intro.html

RESOURCE: Conducting Mobile Surveys Responsibly, World Food Programme (WFP) https://documents.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp292067.pdf

RESOURCE: The Signal Code: A Human Rights Approach to Information During a Crisis, Harvard Humanitarian Initiative https://signalcodeorg.files.wordpress.com/2017/01/signalcode_final7.pdf

RESOURCE: Research Data Security: Protecting Human Subjects' Identifiable Data, University of California, Berkeley, Human Research Protection Program https://cphs.berkeley.edu/policies_procedures/ga106.pdf

RESOURCE: Framework for Creating a Data Management Plan, ICPSR https://www.icpsr.umich.edu/icpsrweb/content/datamanagement/dmp/framework.html

RESOURCE: Data Security, University of California, Berkeley, Committee for Protection of Human Subjects https://cphs.berkeley.edu/datasecurity.pdf