Principe: Assurer la confidentialité et la sécurité

Introduction

Assurer la confidentialité et la sécurité du développement numérique implique une évaluation soigneuse du type de données collectées et de la façon de les acquérir, de les utiliser, de les stocker et de les communiquer. Les organisations doivent prendre des mesures pour minimiser la collecte et protéger les informations confidentielles et les identités des personnes représentées dans les bases de données, contre tout accès non autorisé et toute manipulation par des tiers. Les pratiques responsables des organisations qui collectent et utilisent les données de personnes comprennent le respect de leur nature sensible, la transparence sur la méthode de collecte et d'utilisation, la minimisation de la quantité des informations personnellement identifiables et sensibles, l'élaboration et l'application de politiques de sécurité protégeant les données et respectant la confidentialité et la dignité des personnes, et la création d'une politique de fin de cycle pour la gestion des données post-projet.

Concepts de base

- **Définissez les entités détenant la propriété, la souveraineté et l'accès aux données avant de les recueillir ou de les saisir.** Déterminez les lois et réglementations locales à respecter en matière de protection des données, qui est responsable de l'utilisation des données, qui y a accès ou peut les utiliser, et où les données peuvent (ou doivent) être stockées.
- **Agissez dans le meilleur intérêt des utilisateurs finals et des personnes dont les données sont recueillies.** Tdès la planification, afin de protéger la confidentialité et la sécurité des données et d'assurer une mise en œuvre éthique. Ceci est particulièrement important lorsque les maîtres d'œuvre travaillent avec des communautés vulnérables ou marginalisées qui pourraient ne pas avoir leur mot à dire sur la façon dont leurs données sont collectées, utilisées ou partagées.
- **Effectuez une analyse des risques et des bénéfices des données traitées** pour identifier les bénéficiaires et les

LIGNES DIRECTRICES POUR LE CYCLE DE VIE DU PROJET

Les conseils, recommandations et ressources ci-dessous, fournis par la communauté de développement numérique, vous expliquent les occasions d'appliquer ce principe durant chaque phase du cycle de vie du projet. Ces lignes directrices ne prétendent pas être exhaustives, mais suggèrent des mesures que vous pouvez prendre pour appliquer ce principe à votre travail. Si vous souhaitez ajouter d'autres conseils, recommandations et ressources, veuillez en faire part à la communauté à https://forum.digitalprinciples.org/

personnes vulnérables. Il faut parfois répéter ce processus tout au long du projet parce que de nouvelles données sont nécessaires, de nouveaux risques ont été identifiés ou le partage de données avec de nouveaux partenaires est envisagé.

- **Évaluez les risques** d'un accès non autorisé aux données ou d'une fuite des données stockées. Tenez compte de l'impact potentiel de ces données sur les particuliers si elles sont communiquées ou publiées de façon malveillante, ainsi que des risques si les données sont intégrées dans d'autres séries de données.
- **Comprenez que les risques dépendent hautement du contexte,** pas seulement dans les pays mais également dans les communautés, les populations, ainsi que du moment. Si vous travaillez avec des communautés vulnérables ou marginalisées, quels groupes pourraient avoir intérêt à acquérir vos données et ont la capacité de le faire ? Les contrôles de l'information et de l'accès aux données sont-ils suffisants?
- **Minimisez la collecte des informations personnellement identifiables.** Demandez-vous si les informations personnelles sont cruciales pour la réussite du projet et examinez les conséquences au cas où des tiers y auraient accès, surtout si vous travaillez avec des utilisateurs appartenant à des populations vulnérables (minorités, handicapés, femmes et enfants, par exemple). Prévoyez une évaluation des risques de la collecte d'informations personnelles.
- **Cataloguez et faites un suivi de toutes données à caractère personnel ou sensible recueillies tout au long du projet:** Préparez un plan de destruction ou de stockage sécurisé hors ligne des données sensibles, durant le projet et par la suite. Incluez un contrôle des disques durs, du stockage dématérialisé des fichiers, des clés USB, des boîtes de réception de messages électroniques et d'autres

"Rappelez-vous que les mesures de sécurité techniques sont aussi bonnes que leurs utilisateurs humains. La technique de sécurité doit fonctionner dans le contexte où il est implémenté."

CLAYTON SIMS, DIMAGI

Principe: Assurer la confidentialité et la sécurité

sources fréquentes de fuites de données.

- **Expliquez franchement** aux personnes concernées comment votre initiative utilisera et protégera leurs données.
- **Obtenez le consentement éclairé** avant la collecte des données. Il est crucial de veiller à ce que les participants comprennent pourquoi leurs données sont recueillies, comment elles sont utilisées et partagées, et comment les participants peuvent avoir accès aux données collectées ou les modifier, et qu'ils aient l'option de refuser de participer. Les participants doivent être informés et doivent parfaitement comprendre les risques associés à la communication de leurs données. Des formulaires de consentement doivent être rédigés dans la langue locale et faciles à comprendre pour les personnes dont les données sont recueillies.
- **Protégez les données** en adoptant les meilleures pratiques pour sécuriser les données et en contrôler l'accès. En voici quelques exemples : chiffrement des fichiers, authentification en deux étapes, autorisations limitées d'accès, stockage des données sur des serveurs sécurisés ou des services de stockage en nuage (cloud), et application de politiques et procédures organisationnelles de sécurité, y compris d'accords de partage de données avec tous les partenaires concernés.

Le respect de ces principes est essentiel pour assurer une mise en œuvre conforme à l'éthique des initiatives de développement numérique et pour éviter les préjudices causés par des atteintes à la sécurité. Les pratiques de protection de la confidentialité des informations personnelles et les sauvegardes de sécurité protègent les intérêts de la communauté, tout en renforçant la confiance entre les utilisateurs et les praticiens du développement numérique. Il faut protéger la confidentialité et la sécurité des informations pour préserver la dignité et la sécurité des personnes concernées.

ANALYSE ET PLANIFICATION

CONSEILS ET RESSOURCES

CONSEIL: Adoptez les meilleures pratiques de collecte et de gestion des données privées et des informations sensibles:

- Obtenez le consentement éclairé de la part des propriétaires des données pour les processus utilisés aux fins d'accès, d'utilisation et de communication de leurs informations personnelles.
- Soyez transparents avec les personnes dont l'information est collectée quant à la façon dont vous utiliserez les données.
- Précisez des mécanismes permettant aux particuliers d'accéder aux informations sur les méthodes de collecte et d'utilisation de leurs informations personnelles.
- Collectez les informations personnelles uniquement pour un usage spécifique, équitable et justifié.
- Minimisez la collecte de données et ne relevez que ce qui est absolument nécessaires.
- Appliquez des normes d'accès et suivez les meilleures pratiques en ce qui concerne l'accès aux données, les mises à niveau et la gestion.

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

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

Principe: Assurer la confidentialité et la sécurité

Analyse et planification

Pendant cette phase, réfléchissez de façon stratégique à quelles données collecter et à la manière dont elles seront utilisées tout au long du cycle de vie du projet. Décidez comment assurer la

confidentialité et la sécurité des informations sensibles terminez pendant chaque phase, et évaluez s'il est nécessaire de collecter les données à la lumière des risques d'atteinte

- **Identifiez les données essentielles pour le succès de l'initiative en tenant compte du meilleur intérêt des personnes concernées.** N'oubliez pas que le fait même de collecte des données peut mettre en péril certaines populations vulnérables. Collectez le minimum d'informations personnellement identifiables et de données sensibles et obtenez toujours le consentement éclairé des personnes concernées, au moyen de formulaires compréhensibles rédigés dans la langue appropriée. Examinez si des bases de données anonymes pourraient être combinées pour identifier des utilisateurs spécifiques et leur rapporter les données anonymes confidentielles.
- **Effectuez une évaluation du risque** pour identifier les dangers internes et externes menaçant vos données ainsi que les vulnérabilités du système. Classez les menaces ou vulnérabilités par ordre de priorité, en fonction du préjudice potentiel, du nombre d'utilisateurs touchés, du potentiel d'exploitation et du risque d'atteinte à la réputation. Préparez un plan de gestion du risque décrivant les mesures de prévention prises pour répondre aux menaces de caractère hautement prioritaire.
- **Étudiez les ramifications pour la durabilité ou la mise à l'échelle** pour décider les données à collecter. Il vous faudra peut-être obtenir plus d'informations pour un déploiement généralisé [http://digitalprinciples.org/build-for-sustainability/] [http://digitalprinciples.org/design-for-scale/].
- **Connaissez les règles et règlementations locales en matière de confidentialité et sécurité des données, y compris les règlements des comités de surveillance institutionnels.** Dialoguez avec les agents de la fonction publique, les leaders locaux, les responsables de la réglementation des données (les organisations internationales et les administrateurs d'hôpital, par exemple) et vos utilisateurs [http://digitalprinciples.org/

ANALYSE ET PLANIFICATION

CONSEILS ET RESSOURCES

RESSOURCE: European Union General Data Protection Regulation (EU GDPR). http://www.eugdpr.org/

RESSOURCE: 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

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

CONCEPTION ET ÉLABORATION

CONSEILS ET RESSOURCES

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

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

RESSOURCE: 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

design-with-the-user/]. Connaissez les conséquences en cas de non-conformité (par exemple, pénalités ou sanctions), ainsi que son impact négatif sur la réputation de votre organisation et la réussite de l'initiative.

- **Prévoyez des capacités de surveillance.** Attribuez à des personnes bien précises les responsabilités de gestion de la sécurité et des risques et menez des sessions de sensibilisation au risque et de formation pour les utilisateurs des données. Identifiez et obtenez un financement régulier pour les mesures de sécurité et la surveillance.

Conception et élaboration

Durant cette phase, il faut élaborer, tester et officialiser des plans de gestion et de protection de la sécurité des données. Vous pouvez également collecter des données pour renseigner la conception et le développement des outils numériques utilisés dans le programme.

- **Préparez un plan de gestion des données** avant d'entamer la collecte des données. Le plan de gestion des données décrit en détail ce que vous ferez des données pendant et après la fin de votre initiative pour assurer l'accès aux données et leur sécurité. Répondez aux questions suivantes dans votre plan:
  - **Collecte des données:** Quelle quantité de données seront collectées, pendant combien de temps, et qui a la responsabilité de leur collecte, gestion et sécurité?
  - **Validation et nettoyage:** Le processus de nettoyage des données comprend-il la suppression des informations personnellement identifiables (surtout en ce qui concerne les données qualitatives)?
  - **Organisation et stockage:** Comment allez-vous documenter et enregistrer vos données de façon à que les tiers puissent les comprendre et y avoir accès ? Quels formats de fichiers et quelles conventions de nommage utiliserez-vous ? Et quelles seront vos procédures de stockage pour assurer la sécurité des données?
  - **Accès:** Qui détient les droits aux données ? Comment les données seront-elles communiquées ? Comment protégez-vous les informations personnelles ? Et la réutilisation sera-t-elle autorisée?

CONCEPTION ET ÉLABORATION

CONSEILS ET RESSOURCES

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

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

RESSOURCE: Girl Safeguarding Policy: Digital Privacy, Security, & Safety Principles & Guidelines, Girl Effect. http://www.girleffect.org/media/3052/gem-girl-safeguarding-policys_19-05-16.pdf.

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

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

DÉPLOIEMENT ET MISE EN ŒUVRE

CONSEILS ET RESSOURCES

CONSEIL: Utilisez une liste de contrôle pour la protection des données afin d'assurer leur sécurité. Vous pouvez également utiliser cette liste de contrôle pour créer des indicateurs aux fins de la surveillance et de l'évaluation de la sécurité et de la confidentialité des données.

- Les classeurs sont-ils tous verrouillés et les dossiers papier sont-ils sécurisés?
- Les mots de passe des ordinateurs

Principe: Assurer la confidentialité et la sécurité

- **Archivage:** Pendant combien de temps les données seront-elles conservées ? Comment les données seront-elles supprimées lorsqu'elles ne seront plus nécessaires ? Et comment les données seront-elles anonymisées ? Existe-t-il un service d'archivage à code source ouvert (open source) pour stocker les données ou bien les données seront-elles transférées à une autre organisation?

Veillez à ce votre plan soit conforme aux politiques de l'organisation en matière de confidentialité, de sécurité et de gestion responsable des données et des normes de la communauté des logiciels ouverts, le cas échéant. Communiquez votre plan à vos partenaires, aux utilisateurs cibles et à la communauté du développement numérique dans son ensemble afin de promouvoir la transparence, la responsabilité et la confiance. Assurez-vous que ces différentes parties prenantes puissent comprendre et appliquer le plan.

- **Nommez les membres de l'équipe qui seront chargés de la gestion et de la sécurité des données tout au long du cycle de vie du projet.** Les responsabilités sont les suivantes : modifier le plan de gestion des données en cas d'évolution de l'environnement externe, effectuer une analyse des risques, contrôler les données pour assurer leur sécurité et répondre aux atteintes à la sécurité, ainsi qu'organiser la formation des personnes qui deviendront propriétaires des données de l'initiative en cas de leur transfert.
- **Menez également régulièrement un examen des fonctionnalités du système qui saisissent automatiquement les données.** Pendant la phase de développement, de nouvelles fonctions peuvent être ajoutées pour la saisie des données dans le système. L'initiative justifie-t-elle la saisie de ces données et existe-t-il des politiques bien claires pour la collecte, le stockage, l'utilisation et l'élimination des données.
- **Développez l'outil numérique de manière à respecter les normes actuelles de sécurité informatique et matérielle des données personnelles.** Par exemple, veillez à ce que la plateforme utilisée par votre initiative puisse gérer l'accès des utilisateurs aux données et les autorisations d'affichage ou d'utilisation des données.

DÉPLOIEMENT ET MISE EN ŒUVRE

CONSEILS ET RESSOURCES

sont-ils robustes

- Des numéros d'identification anonymes ont-ils été attribués à tous les participants à l'étude?
- Tous les membres du personnel ont-ils suivi une formation sur la confidentialité et le respect de la vie privée ?
- Tous les fichiers de sauvegarde sont-ils sécurisés?
- Dans quelles circonstances les données peuvent-elles être communiquées et à qui ? Comment communiquer les données en toute sécurité?
- Les procédures de sécurité sont-elles régulièrement revues et mises à jou?
- Ne stockez pas de données sur des clés USB ou autres périphériques externes, aisément volés ou perdus.
- N'envoyez pas d'informations personnellement identifiables dans des courriers électroniques.

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

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

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

Principe: Assurer la confidentialité et la sécurité

Déploiement et mise en oeuvre

Pendant cette phase, mettez en œuvre de plan de gestion des données. En fonction de l'initiative, il se peut que vous collectiez des informations personnelles. Expliquez régulièrement quelles sont les données que vous recueillez, comment elles sont utilisées, par qui, et comment elles sont sécurisées.

- **Contrôlez l'accès aux données pour protéger leur intégrité et leur confidentialité.** Créez des groupes d'accès détenant des autorisations spécifiques en fonction du rôle des utilisateurs. La règle générale devrait être des autorisations aussi limitées que possible pour la plupart des personnes, et de ne pouvoir accorder d'autres autorisations (comme for accès en lecture/écriture) qu'aux utilisateurs essentiels. Exigez des mots de passe personnels pour tous les utilisateurs et envisagez l'authentification en deux étapes. L'authentification en une étape exige uniquement le nom d'utilisateur et un mot de passe pour accéder à un compte. L'authentification en deux étapes ajoute une exigence après la saisie du mot de passe, comme la réception sur le numéro de téléphone associé au compte d'un SMS comportant un code de vérification, qui doit alors être entré pour accéder au compte.
- **Mettez en place des mesures de prévention contre les risques et vulnérabilités prioritaires.** Effectuez régulièrement des analyses de risque et des contrôles de sécurité pour repérer les vulnérabilités émergentes. Intervenez immédiatement en cas d'atteinte à la sécurité pour en minimiser rapidement et facilement les effets négatifs, et en informer les personnes concernées.
- **En cas de clôture du projet, exécutez le plan de destruction des données ou de transfert pour stockage à long terme.** Détruisez toutes les données jugées sensibles ou qui ne sont pas nécessaires pour les initiatives futures ou l'évaluation. Expliquez aux parties prenantes concernées comment les données sont gérées ou détruites.
- **En cas de mise à l'échelle ou de transfert, travaillez avec les nouveaux membres ou les nouvelles organisations de l'initiative pour vous assurer de bien comprendre et de respecter le plan en place de gestion des données.** Repérez les insuffisances de sécurité pouvant découler de la

SUIVI ET ÉVALUATION INTERSECTORIELS

CONSEILS ET RESSOURCES

- CONSEIL: Une bonne organisation des données d'étude (et d'autres activités) exige d'utiliser systématiquement des codes d'identification tout au long des processus de collecte et de saisie des données. Les codes d'identification permettent de retracer et de relier toutes les données, quelle que soit leur origine
- RESSOURCE: The Hand-Book of the Modern Development Specialist: Sharing Data, Responsible Data Forum. https://responsibledata.io/resources/handbook/chapters/chapter-02c-sharing-data.html.
- RESSOURCE: Ethical Guidelines for Educational Research, British Educational Research Association (BERA). https://www.bera.ac.uk/researchers-resources/publications/ethical-guidelines-for-educational-research-2011
- RESSOURCE: Research Ethics Training Curriculum, FHI360. https://www.fhi360.org/sites/all/libraries/webpages/fhi-retc2/RETCTraditional/intro.html.
- RESSOURCE: Conducting Mobile Surveys Responsibly, World Food Programme (WFP). http://documents.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp292067.pdf.
- RESSOURCE: 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
- RESSOURCE: Research Data Security: Protecting Human Subjects' Identifiable Data, University of California, Berkeley, Human Research Protection Program. http://cphs.berkeley.edu/

mise à l'échelle ou du transfert. Collaborez avec les partenaires pour corriger les insuffisances et modifier le plan de gestion des données.

Suivi et évaluation intersectoriels

Respectez toujours votre plan de gestion des données, en apportant les modifications nécessaires en fonction des conclusions du suivi-évaluation

- **Préparez un plan de collecte des données compatible avec votre plan de suivi et d'évaluation,** et reflété dans votre plan de gestion des données. Assurez-vous que tout le personnel ait appris à exécuter le plan et que tous les responsables du recueil des données aient suivi une formation sur l'éthique de la recherche. FHI360 propose un programme de formation gratuit en matière d'éthique de la recherche à l'intention des professionnels du développement international [https://www.fhi360.org/sites/all/libraries/webpages/fhi-retc2/RETCTraditional/intro.html].

- **Appliquez les éléments de votre plan de gestion des données concernant l'organisation des données, le stockage et l'accès.** Après leur recueil, veillez à ce que les données soient conservées en toute sécurité tout en restant accessibles. Réfléchissez aux questions suivantes:
  - Comment le système de gestion des fichiers est-il organisé et hiérarchisé?
  - Où résident les métadonnées du système de gestion des fichiers (y compris le plan de gestion des données) ?
  - Quel système de nommage des fichiers allez-vous utiliser?
  - Combien de copies des fichiers seront stockées dans la base de données électronique?
  - Une technologie réseau sera-t-elle utilisée pour stocker les fichiers (par exemple, un lecteur partagé ou un stockage en nuage)?
  - Comment les données seront-elles archivées?
  - Comment les données archivées seront-elle protégées (par exemple, base de données verrouillée)?
  - De combien d'espace de stockage faudra-t-il disposer pour les fichiers ? Cet espace est-il disponible ou faudra-t-il l'acheter?

- **Faites attention aux risques pour la confidentialité des personnes et supprimez toutes les informations personnellement**

SUIVI ET ÉVALUATION INTERSECTORIELS

CONSEILS ET RESSOURCES

policies_procedures/ga106.pdf

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

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

identifiables. Utilisez des codes d'identification pour toute la collecte de données et tout le processus de saisie de données pour pouvoir effectuer un suivi des réponses dans le respect de la confidentialité. Ceci est particulièrement important pour les populations vulnérables ou marginalisées. Sachez que la fusion de séries de données peut réidentifier les personnes.

- **Évaluez en permanence les risques pour les données et les vulnérabilités du système.** Veillez à ce que le plan de gestion du risque soit systématiquement appliqué
- **Réfléchissez aux questions d'ordre éthique plus générales.**
- **Surveillez les indicateurs relatifs à la sécurité et à la confidentialité des données.** La liste de vérification pour la sécurité des données fournie dans *Conseils et ressources pour le déploiement et mise en œuvre* propose plusieurs indicateurs possibles.