OUTIL N°2

PACK RH EN GESTION DES DONNÉES PROGRAMMES À DESTINATION DES OSC DE SOLIDARITÉ INTERNATIONALE

REFERENTIEL METIERS EN PRATIQUE

BLOC DE COMPETENCES 5 : ORGANISER ET METTRE EN ŒUVRE DES APPROCHES ASSURANT UNE GESTION RESPONSABLE DES DONNEES

cartong

AOUT 2022

CARTONG

Créée en 2006, CartONG est une ONG française support spécialisée en gestion de l'information qui a vocation à mettre la donnée au service des projets humanitaires, de développement et d'action sociale. Nous cherchons à améliorer la qualité et la redevabilité des activités terrain, notamment par une meilleure évaluation des besoins et par un meilleur suivi/évaluation. En tant que centre de ressources et d'expertises pluridisciplinaire, nous accompagnons les stratégies et les opérations de nos partenaires. Nos équipes soutiennent également le secteur en produisant de la documentation, en renforçant les capacités et en sensibilisant aux défis techniques, stratégiques et éthiques des technologies numériques.

REMERCIEMENTS

La présente publication bénéficie du soutien de l'Agence Française de Développement (AFD) et du Centre de crise et de soutien du Ministère de l'Europe et des Affaires étrangères (CDCS). Néanmoins, les idées et les opinions présentées dans ce document ne représentent pas nécessairement celles de l'AFD ou du CDCS.

1. COMPETENCES AU SEIN DU BLOC

C5.1 : Connaître et mettre en œuvre des procédures et pratiques en protection des données assurant une conformité avec la législation nationale et internationale.

C5.2 : Connaître et appliquer les principes éthiques de gestion responsable des données en prenant en compte les bonnes pratiques du secteur et les spécificités contextuelles.

C5.3 : Définir et mettre en œuvre les bonnes pratiques en sécurisation de données.

2. L'OBJECTIF COMMUN DE CES COMPETENCES

L'ensemble de ces compétences vise à garantir une **gestion responsable des données** via la mise en œuvre de **bonnes pratiques, le respect des standards et des principes** en application dans le secteur de l'humanitaire et du développement international ainsi que le respect du **cadre juridique national et international** relatif aux données personnelles.

Les compétences composant le bloc de compétences n°5 sont nécessaires lorsque les équipes programme [et S&E] collectent la moindre donnée sur les populations vulnérables. De telles compétences sont nécessaires pour déterminer si les données collectées sont personnelles et/ou sensibles afin de pouvoir mettre en œuvre les mesures pour assurer une gestion éthique des données notamment via une sécurisation adaptée des données et assurer la conformité avec les cadres légaux, et standards du secteur. En fonction des contextes, ces compétences peuvent être réparties autour de personnes n'étant pas directement connectées aux données programmes tels que les postes de DPO, relai local DPO, Coordinateurs·rices Terrain, IT, etc.

3. LES SAVOIR-FAIRE ASSOCIES ET LEUR APPLICATION

C5.1 : CONNAÎTRE ET METTRE EN ŒUVRE DES PROCÉDURES ET PRATIQUES EN PROTECTION DES DONNÉES ASSURANT UNE CONFORMITÉ AVEC LA LÉGISLATION NATIONALE ET INTERNATIONALE

Compétence 5.1

Niveau de maîtrise	Savoir-faire techniques	Savoir-faire méthodologiques
	Différencier des données personnelles ou sensibles. Exécuter des directives claires pour la protection des données (configuration d'outils, recueil de consentement, exécution du protocole d'archivage, ou dé-identification, anonymisation, pseudonymisation, agrégation etc.).	N/A

	Connaître et faire appliquer les éléments clés de la réglementation relative à la protection des données à l'international (RGPD etc.). Connaître et faire appliquer les éléments clés de la réglementation relative à la protection des données du ou des pays d'intervention tels que par exemple les principes de limitation de traitement, de conservation limitée, de proportionnalité, les droits des personnes concernées etc. Appliquer des mesures de protection des données, dès la conception et la protection des données par défaut, par exemple dans le choix et la configuration d'outils de gestion des données, dans la conception de formulaires de collecte etc.	Analyser succinctement une législation. Concevoir et mettre en œuvre des actions de sensibilisation et de formation. Identifier les points d'action pour améliorer la protection des données programmes. Adapter les mesures préconisées aux contextes d'intervention. Mettre en place des pratiques, procédures et méthodologies permettant de mettre en œuvre les grands principes de la protection des données par exemple : • Choix d'une base légale, • Recueil du consentement éclairé, • Choix d'une durée de rétention, • Mise en place de protocole d'archivage, dé-identification, anonymisation, Pseudonymisation, agrégation, etc.

	Connaître précisément la législation internationale et nationale en matière de protection des données. Mettre en place des pratiques, procédures et méthodologies permettant d'assurer la protection des données sur l'ensemble des composants, par exemple : • Rédaction d'accords de partage de données, • Evaluation d'un sous-contractant. Rédiger ou revoir les contrats ou accords type DTA/DSA. Réaliser et rédiger un DPIA (Analyse d'impact relative à la protection des données) sur un traitement de données ou un projet simple, impliquant peu de parties prenantes ou peu de solutions techniques. Assurer le suivi contractuel des partenaires et bailleurs sur la dimension protection des données.	Etablir un diagnostic et mettre en œuvre un plan d'action pour assurer la conformité avec les législations nationales et internationales. Analyser la conformité d'un traitement et mettre en évidence des non-conformités. Élaborer la stratégie d'une mission ou organisation en matière de protection des données. Concevoir et diffuser des pratiques, procédures et méthodologies permettant de mettre en œuvre les grands principes de la protection des données.
	Réaliser et rédiger un DPIA (Analyse d'impact relative à la protection des données) sur un traitement de données au niveau d'une mission ou d'une organisation, complexe impliquant une grande variété de solutions et de parties prenantes.	N/A

Dans quelle situation la compétence C5.1 est-elle mobilisée ?	
En générale la compétence C5.1 est mobilisée	Dès lors que des données sur les populations vulnérables sont collectées…
Et plus spécifiquement pour le niveau A 	…et lorsqu'il est uniquement nécessaire d'identifier si celles-ci sont sensibles ou personnelles afin d'appliquer les mesures adaptées. Ou bien lorsque des directives claires et appliquées aux collectes spécifiques de l'organisation existent et il "suffit" de les appliquer. Une

	personne relai spécialisée protection des données existe au niveau local pour accompagner ce niveau.
Et plus spécifiquement pour le niveau B 	…et lorsque des lignes directrices générales existent au sein de l'organisation, et qu'il est nécessaire de les adapter aux activités de collecte spécifiques. …et/ou lorsqu'une personne relai spécialisée en protection des données existe au niveau international.
Et plus spécifiquement pour le niveau C 	…et lorsqu'il est nécessaire de conduire un diagnostic de la conformité avec les lois en vigueur. …et lorsque les lignes directrices de l'organisation sont à rédiger ou à mettre à jour.
Et plus spécifiquement pour le niveau D 	…et lorsqu'il est nécessaire de conduire une analyse d'impact relative à la protection des données dans un environnement complexe.

C5.2 : CONNAÎTRE ET APPLIQUER LES PRINCIPES ÉTHIQUES DE GESTION RESPONSABLE DES DONNÉES EN PRENANT EN COMPTE LES BONNES PRATIQUES DU SECTEUR ET LES SPÉCIFICITÉS CONTEXTUELLES

Compétence 5.2

Niveau de maîtrise	Savoir-faire techniques	Savoir-faire méthodologiques
	Adopter les standards de protection des données appliqués à la solidarité internationale (Code éthique type Signal, *Principles for Digital Development* etc.) et au contexte (groupes armés non étatiques, données médicales etc.).	Identifier les enjeux éthiques clés d'un traitement de données ou d'un projet et alerter en cas de doute ou d'identification d'un risque (par exemple bloquer un transfert de données en l'absence d'analyse de risque). Assurer l'appropriation par les équipes programmes des enjeux éthiques (techniques de sensibilisation et formation).

	Appliquer les directives bailleurs en termes de protection des données.	
	N/A	Identifier les enjeux de débat liés à l'application des concepts et lois de protection des données dans le secteur de la solidarité internationale : • Notion de gestion responsable vs. Protection, • Application du consentement éclairé, inadaptation du RGPD au contexte d'intervention. Évaluer en profondeur les enjeux éthiques d'un traitement de données ou d'un projet (être en capacité d'argumenter indépendamment pour refuser le transfert de données à une organisation partenaire, évaluer le degré de risque d'une collecte de données etc.). Etablir un diagnostic et mettre en œuvre un plan d'action pour entrer en conformité avec les principes éthiques.

Dans quelle situation la compétence C5.2 est-elle mobilisée ?	
En générale la compétence C5.2 est mobilisée	Dès lors que des données sur les populations vulnérables (personnelles et sensibles) sont collectées…
Et plus spécifiquement pour le niveau B 	…et qu'il est nécessaire d'adapter les activités de collecte spécifiques aux lignes directrices générales, existantes au sein de l'organisation (pour la mise en conformité avec les standards définis par les bailleurs et le secteur).

Et plus spécifiquement pour le niveau C 	…et lorsqu'il est nécessaire de conduire un diagnostic de la conformité avec les lignes directrices fixées par les bailleurs et les standards du secteur. …et lorsque les lignes directrices de l'organisation sont à rédiger ou à mettre à jour.

C5.3 : Définir et mettre en œuvre les bonnes pratiques en sécurisation de données

Compétence 5.3

Niveau de maîtrise	Savoir-faire techniques	Savoir-faire méthodologiques
	Pré-identifier les types de données ayant besoin d'être protégées (sensibles, personnelles, données communautaires). Avoir des réflexes de sécurisation simple des données papiers et numériques : armoire fermée, bien choisir un mot de passe, cryptage d'un fichier, partage de données en interne et externe etc. Connaître les bonnes pratiques de sécurisation des différents outils utilisés.	N/A
	Mettre en place une sécurisation des données papiers et numériques à l'échelle d'un projet (cryptage d'un cloud partagé, modalité de partage de mot de passe, choix d'une méthode d'authentification, gestion des accès utilisateur, mesures de traçabilité, évaluation de la force d'un mot de passe, modalité de back-up, méthode d'anonymisation et de pseudonymisation, etc.). Connaître l'ensemble du panel de composants de la sécurité des données (notamment des méthodes de sécurisation des différents outils utilisés).	Adapter les lignes directrices de l'organisation à des contextes spécifiques et rédiger des guides de pratiques standards. Diffuser et savoir s'assurer de la mise en œuvre de procédures.
	Réaliser des audits "basiques" en sécurisation des données. Connaître de manière approfondie les différentes composantes de sécurisation technique et organisationnelle des données et des degrés afférents à chacun : • Différence entre cryptage pendant le transfert vs. pendant le stockage,	Concevoir et harmoniser les pratiques de sécurisation des données au sein de l'organisation. Évaluer le niveau de sécurisation des données mis en place dans un projet ou une organisation ou d'un partenaire (évaluer les pratiques, juger de la pertinence et

	• Certification de serveur, notion de clé PGP ou standard AES etc.	adéquation du choix des mesures). Être en capacité de communiquer avec aisance avec des équipes informatiques en cybersécurité.
	Connaître de manière approfondie l'environnement informatique de l'organisation et les bonnes mesures de cybersécurité associées. Appliquer des mesures avancées de sécurisation des données dans un environnement complexe (partenaires, outils et localisation multiple). Réaliser des audits complets en matière de sécurisation des données.	N/A

Dans quelle situation la compétence C5.3 est-elle mobilisée ?	
En générale la compétence C5.3 est mobilisée	Dès lors que l'organisation utilise des outils informatiques et numériques pour la collecte, la gestion et le stockage des données…
Et plus spécifiquement pour le niveau A 	…et lorsqu'il est nécessaire d'exécuter les manipulations de sécurisation des données sur les outils.
Et plus spécifiquement pour le niveau B 	…et lorsque qu'il est nécessaire de coordonner les pratiques de sécurisation des données, d'assurer leur mise en application sur l'ensemble d'une mission.
Et plus spécifiquement pour le niveau C 	…et lorsqu'il est nécessaire d'établir les orientations stratégiques en termes de sécurisation des données, de vérifier leur bonne application et d'assurer la coordination avec les services associés.
Et plus spécifiquement pour le niveau D 	…et lorsqu'il est nécessaire de mettre en place un système complexe (partenaires, localisation, et outils informatiques et numériques multiples) de sécurisation des données.

4. CE QU'IL FAUT GARDER A L'ESPRIT LORS D'UN RECRUTEMENT

Formation

Formation dédiée à la protection des données : double parcours en technologie de l'information (pour pouvoir interagir facilement avec le personnel IT) et droit/juridique.

Expérience

Data Protection, mise en place d'un cadre de conformité RGPD.

Maîtrise de concepts et outils clés

Basique	Intermédiaire	Avancée
• Données sensibles • Données personnelles • Données communautaires • Mots de passe / gestion des accès • "Ne pas nuire" (*Do no Harm*) • Consentement • Gestion responsable des données vs. Protection des données	• Concepts généraux de la RGPD (base légale d'application de la protection des données) • Cryptage (en transit et pendant le stockage) • Pratique de dé-identification, anonymisation, pseudonymisation, agrégation, gestion de périodes de rétention des données • Protection des données par défaut dès la conception ("*by design and by default*")	• Connaissances détaillées de la RGPD, • Connaissances détaillées des règles bailleurs • Accord de partage de données • DPIA • Cyber-sécurité • Certification de serveur (notion de clé PGP ou standard AES…)

Attitudes

- Proactivité, identification des manquements
- Capacité à challenger les besoins de collecte
- Force de proposition (solutions)
- Indépendance, confidentialité, discrétion
- Communication et pédagogie
- Objectivité, impartialité

cartong

23 Boulevard du Musée
73000 Chambéry (France)
+33 (0)4 79 26 28 82

INFO@CARTONG.ORG
WWW.CARTONG.ORG