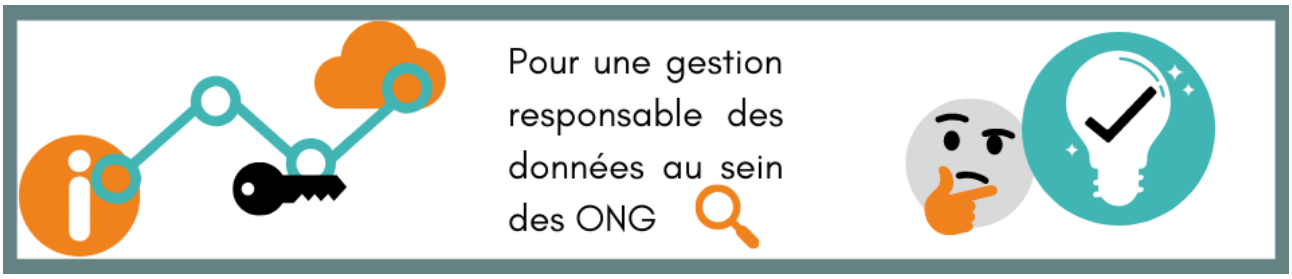


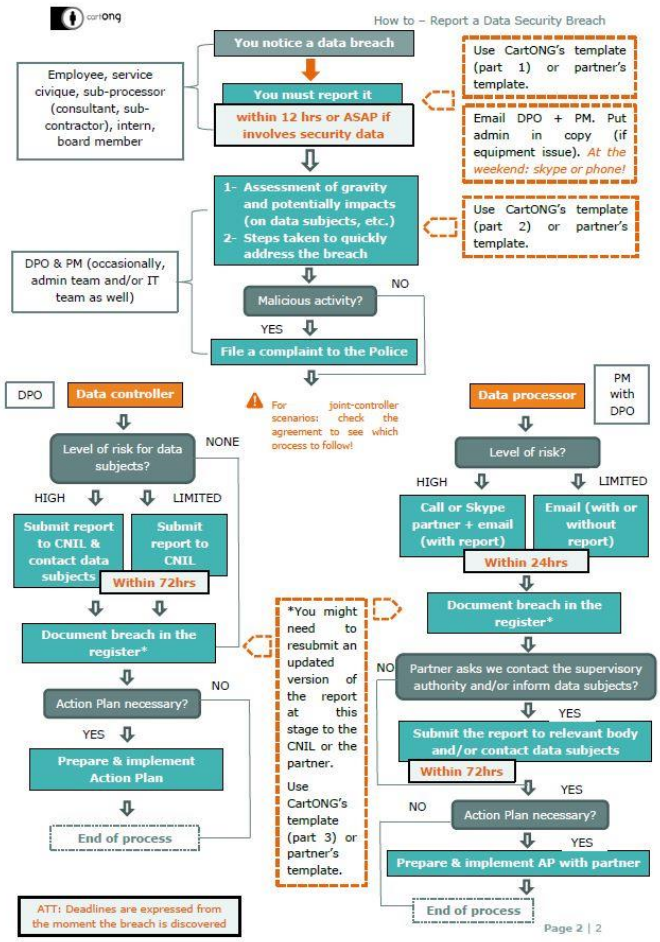
POUR UNE GESTION RESPONSABLE DES DONNÉES AU SEIN DES ONG : 6 APPRENTISSAGES-CLÉS TIRÉS DE L'EXPÉRIENCE DE CARTONG

Comment convaincre ses collègues, les dirigeants de sa structure, ses partenaires, les acteurs du secteur que oui, une gestion responsable des données est non seulement nécessaire mais aussi possible au sein des organisations humanitaires et de développement ? Qu'il n'y a pas que dans les secteurs médicaux, bancaires ou sécuritaires que les données peuvent devenir une arme redoutable et que nous avons une responsabilité accrue en tant qu'ONG ? Que derrière les emails de type "voici ce que nous faisons pour vous en matière de protection des données" envoyés à tout va depuis 18 mois, se cache – ou devrait se cacher – en réalité des changements profonds de pratiques et de processus au sein des organisations, et que tout changement s'il est bien source de contraintes fait aussi naître des opportunités ? Que même si les graphiques résumant les enjeux de la protection des données ressemblent plutôt généralement à cela (attention aux yeux !), ce sujet est abordable par tous si on choisit les bons formats et les bonnes approches ? Qu'il ne faut pas s'inquiéter de la quantité conséquente de changements à implémenter et que, comme tout processus de changement complexe qui se respecte, la première chose est de savoir prioriser ? Autant de questionnements auxquels CartONG a été largement confronté ces deux dernières années.

Mise en place du chiffrement sur les outils de collecte de données sur mobiles, conception de bases de données contenant des informations sensibles, cartographie de maladies stigmatisantes, développement d'applications web contenant des données personnelles : la protection des données est une préoccupation de longue date à CartONG ! Avec l'introduction du RGPD en 2018, notre structure a cependant décidé qu'il était temps de passer à l'étape supérieure et a lancé un vaste processus d'institutionnalisation des principes de gestion responsable des données en interne. Nous vous invitons à découvrir les principales étapes de ce cheminement – toujours en cours – via une actualité publiée sur notre site internet et les leçons que nous en avons tirées dans ce post de blog.

Le travail engagé depuis 18 mois à CartONG nous a en effet permis de dégager quelques retours clés sur les étapes que nous avons déjà parcourues. Ces derniers ne sont pas forcément révolutionnaires mais viennent conforter les premières leçons apprises sur le sujet partagées par d'autres acteurs du secteur.

I. La force du collectif



CartONG a délibérément fait le choix de retarder quelque peu la nomination d'un DPO au profit pendant un an et demi d'une structure collective rassemblée sous la force d'une "task force". En effet, le changement de pratiques et de culture qu'induit l'intégration des principes d'une gestion responsable des données sont tels qu'il est illusoire de vouloir ou faire mener ceux-ci par une seule personne. Si un responsable de projet ou chef d'orchestre est naturellement nécessaire, il est vital que ce dernier puisse s'appuyer sur un réseau de relais tant à la fois pour toucher l'ensemble des départements d'une organisation, démultiplier la force de sensibilisation et la capacité d'alerte en cas de doute sur une activité mais également pour que les équipes disposent d'un premier niveau de réponse capable de les soutenir immédiatement au besoin. Dans le cas de CartONG, ces "points focaux" ont également permis de répartir la charge de travail lié à la rédaction de nouveaux documents (procédures, politiques, etc. – un exemple ci-contre, que vous pouvez trouver au format PDF dans le dossier .zip) et d'adapter ces derniers au plus proche des besoins des différentes équipes techniques.

Notre conseil ? Passer autant de temps que nécessaire afin d'avoir des relais convaincus par le sujet, à l'écoute des préoccupations de leurs collègues et capable de répondre aux interrogations du quotidien. Cela sera une des clés pour que les sessions de formation d'équipe – classiquement réalisées dans le cadre d'un processus d'accompagnement au changement – aient des effets durables !

II. La plus-value d'un support externe

Le recours à une consultance externe a été important pour CartONG, non seulement du fait qu'il est très difficile de maîtriser de manière suffisante en interne – notamment pour une petite organisation comme la nôtre – tous les aspects de la protection des données (cette dernière demandant des compétences tant juridiques qu'en cyber-sécurité par exemple et ce dans des domaines très variés : ressources humaines, relations partenariales, développement web etc.) mais également parce que le recours à un tiers externe expérimenté est un facteur de succès dans une stratégie de changement. Il est ainsi certain que sans cette consultance, nous n'aurions pas avancé aussi rapidement ni été en capacité de déployer de manière aussi qualitative les premiers éléments de mise en conformité.

Notre conseil ? Trouvez un (ou plusieurs) prestataire au plus proche de votre cœur de métier et capable d'être en position "d'accompagnement", c'est à dire à même de répondre à vos diverses questions et interrogations qui émergent au quotidien et à même de vous accompagner dans le processus d'internalisation des compétences nécessaires.

III. L'importance de la phase de diagnostic

Le sujet de la protection des données étant tellement vaste, il est courant d'avoir le sentiment de se "noyer" et de ne pas savoir par où commencer. Dans ce contexte, être en mesure de repérer ses forces et faiblesses peut sembler évident, mais sans un travail approfondi de diagnostic, il est en réalité difficile de réellement identifier les actions à mener et de prioriser ces dernières. Ainsi, si nous avions prévu de manière assez banale – dans le cadre de la consultance – la réalisation d'un rapide état des lieux des pratiques de CartONG, nous avions sous-estimé son importance et son impact. Ce dernier a ainsi non seulement permis d'identifier de nombreux éléments que nous avions clairement sous-estimés (les transferts de données extra-européens par exemple, rares mais existants à CartONG), de prioriser des éléments qui nous semblaient peu urgents dans nos contextes d'intervention (telle que la refonte de notre charte informatique) ou au contraire de relativiser l'importance de certaines actions (comme l'adaptation de certains aspects RH qui se sont avérés moins critiques qu'initialement prévus).

Notre conseil ? Ne vraiment pas négliger la phase de diagnostic – si vous n'étiez pas encore convaincu.

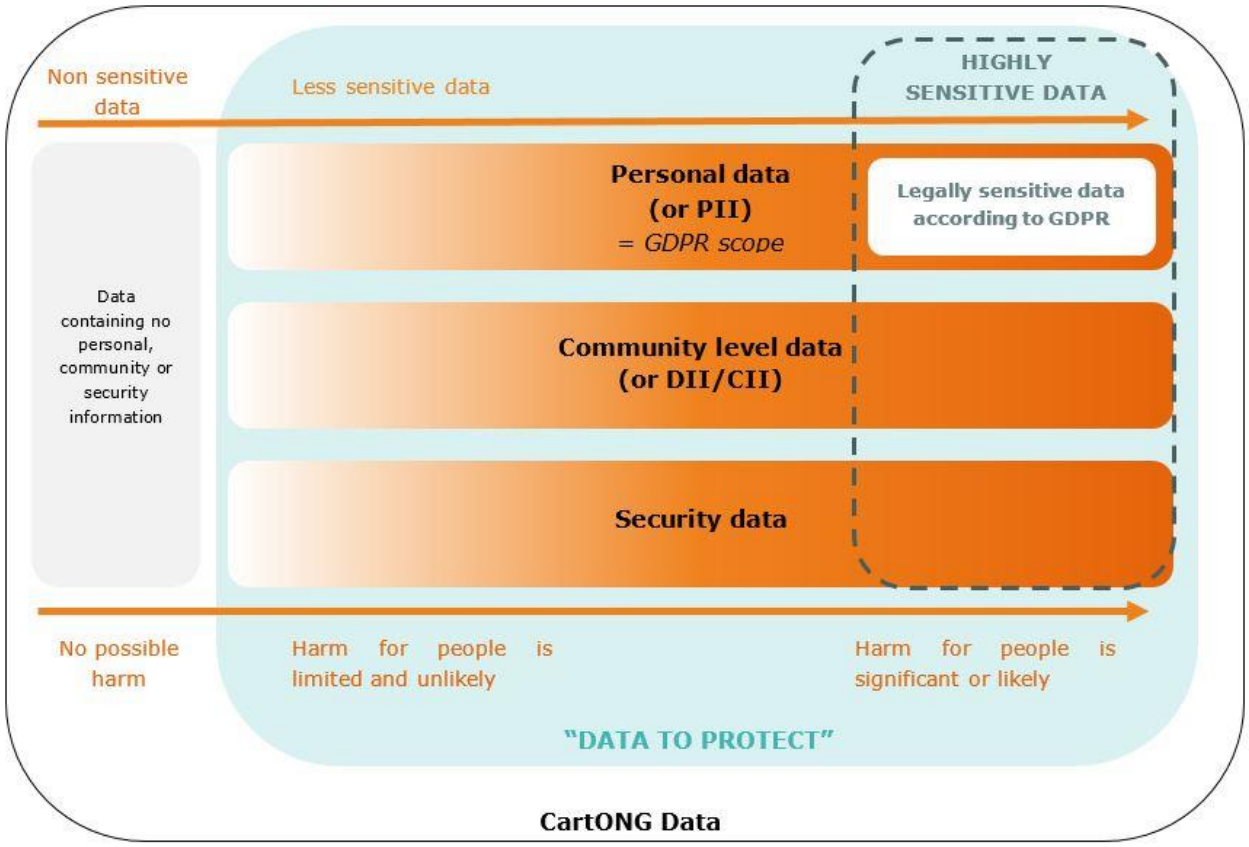
IV. Un travail de très longue haleine

La mise en conformité et l'intégration complète des principes de gestion responsable des données demeurent des tâches de longue haleine, notamment pour une petite structure associative de la taille de CartONG. Le travail initié en 2019 n'en ainsi qu'un début et les efforts devront naturellement se poursuivre au cours des prochaines années sur l'ensemble des axes mentionnés ci-dessus.

Notre conseil ? Ne cherchez pas la mise en conformité absolue et encore moins immédiate ! Mieux vaut prioriser les actions ayant le plus d'impact pour les personnes concernées et aller étape par étape en ne négligeant pas la mise en pratique plutôt que d'avoir une simple conformité de façade.

V. La gestion responsable des données n'est pas qu'une question de RGPD

Dans notre secteur, il est vital de rappeler que la portée de la question de la protection des données ne se limite pas à des enjeux juridiques de mise en conformité au RGPD. Non seulement il s'agit d'un sujet clé d'un point de vue éthique pour les actions humanitaires et de développement afin de "ne pas nuire" à l'ère du numérique (intégration du principe de "do no harm" a la gestion des données – cf. engagement numéro 3 de la norme humanitaire fondamentale) mais également et surtout d'une question de respect des droits et de la dignité des populations que l'on cherche à aider. A cet effet, il est important de ne pas restreindre l'étendue de l'approche aux seules définitions juridiques du RGPD mais d'inclure, à l'instar de la majeure partie des acteurs moteurs sur ce sujet, toute les données qui pourraient être préjudiciables à des personnes ou des organisations. Cela inclut par conséquent, entre autres, les données communautaires agrégées. CartONG a délibérément fait ce choix là en conceptualisant une approche élargie "des données à protéger" dans le cadre de nos activités (vous pouvez trouver ce schéma dans le dossier .zip).

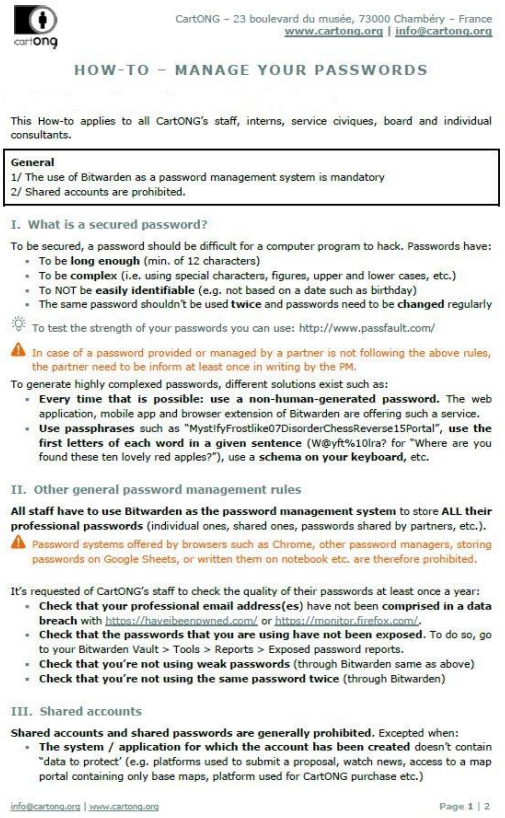


Gestion responsable des données vs. Protection des données

La gestion responsable des données est un concept de plus en plus répandu dans le secteur de la solidarité internationale. D'après OCHA, il va ainsi au-delà des concepts de "confidentialité des données" et/ou de "protection des données" et implique un ensemble de principes, de processus et d'outils qui soutiennent la gestion sûre, éthique et efficace des données dans les interventions humanitaires. Voir également : https://responsibledata.io/what-is-responsible-data/

Notre conseil ? La compréhension de la complexité de la notion de "sensibilité d'une donnée" est clé dans le processus de sensibilisation des équipes (notamment via des outils de type d'analyse d'impact ou DPIA). Chacun voudrait avoir évidemment une classification simple permettant de ranger chaque type de données dans une case une bonne fois pour toute, alors que cela ne fait en réalité aucun sens pour une ONG travaillant à l'échelle mondiale, dans des centaines de contextes différents et évoluant rapidement.

VI. La protection des données peut aussi simplifier la vie !



CartONG – 23 boulevard du musée, 73000 Chambéry – France
www.cartong.org | info@cartong.org

HOW-TO – MANAGE YOUR PASSWORDS

This How-to applies to all CartONG's staff, interns, service civiques, board and individual consultants.

General
1/ The use of Bitwarden as a password management system is mandatory
2/ Shared accounts are prohibited.

I. What is a secured password?

To be secured, a password should be difficult for a computer program to hack. Passwords have:
- To be **long enough** (min. of 12 characters)
- To be **complex** (i.e. using special characters, figures, upper and lower cases, etc.)
- To NOT be **easily identifiable** (e.g. not based on a date such as birthday)
- The same password shouldn't be used **twice** and passwords need to be **changed** regularly

To test the strength of your passwords you can use: http://www.passfault.com/

In case of a password provided or managed by a partner is not following the above rules, the partner need to be inform at least once in writing by the PM.

To generate highly complexed passwords, different solutions exist such as:
- **Every time that is possible: use a non-human-generated password.** The web application, mobile app and browser extension of Bitwarden are offering such a service.
- **Use passphrases** such as "Myst!fyFrostlike07DisorderChessReverse15Portal", **use the first letters of each word in a given sentence** (W@yft%10lra? for "Where are you found these ten lovely red apples?"), use a **schema on your keyboard**, etc.

II. Other general password management rules

All staff have to use Bitwarden as the password management system to store **ALL their professional passwords** (individual ones, shared ones, passwords shared by partners, etc.).

Password systems offered by browsers such as Chrome, other password managers, storing passwords on Google Sheets, or written them on notebook etc. are therefore prohibited.

It's requested of CartONG's staff to check the quality of their passwords at least once a year:
- **Check that your professional email address(es)** have not been **comprised in a data breach** with https://haveibeenpwned.com/ or https://monitor.firefox.com/.
- **Check that the passwords that you are using have not been exposed.** To do so, go to your Bitwarden Vault > Tools > Reports > Exposed password reports.
- **Check that you're not using weak passwords** (through Bitwarden same as above)
- **Check that you're not using the same password twice** (through Bitwarden)

III. Shared accounts

Shared accounts and shared passwords are generally prohibited. Excepted when:
- **The system / application for which the account has been created** doesn't contain "data to protect' (e.g. platforms used to submit a proposal, watch news, access to a map portal containing only base maps, platform used for CartONG purchase etc.)

info@cartong.org | www.cartong.org Page 1 | 2

Enfin, la protection des données n'est pas seulement synonyme de nouvelles contraintes ou de nouvelles procédures pour les équipes. Elle peut aussi tout à fait être l'occasion d'opportunités de simplification ou de clarification de certains processus (tel que l'archivage) voir même d'amélioration réelle du quotidien. A CartONG, le déploiement d'un outil sécurisé mais aussi très pratique et très intuitif pour la gestion des mots de passe – tel que Bitwarden – fut un élément clé d'adhésion et plus personne ne souhaite désormais revenir aux anciens outils.

Vous pouvez trouver ce document eu format PDF dans le dossier .zip.

Notre conseil ? Ne négligez surtout pas les investissements pouvant simplifier la vie des équipes et "dé-diaboliser" autant que possible le sujet en mettant à disposition des outils répondant à leurs contraintes.

Quelques ressources et autres lectures clés que nous recommandons aux acteurs du secteur :

Le manuel sur la protection des données dans l'action humanitaire du CICR

La communauté "Responsible Data" (et notamment sa liste de diffusion/email) coordonné par The Engine Room

Le travail réalisé par HumData (OCHA) via la conception de guides et note techniques : https://centre.humdata.org/data-policy/

L'étude sur la mise en conformité au RGPD des organisations de la société civile (OSC) récemment publié par l'Open Society Foundations. Ce rapport présente les opportunités et défis rencontrés par les OSC et propose également un guide de bonnes pratiques pour limiter les risques.