Gestion responsable des données :
Manuel des formateurs

Contenu

À propos de ce manuel

Ce document a été élaboré dans le cadre du projet GATE (Global Anti-Torture Evidence) de l'IRCT, généreusement financé par le Ministère des Affaires Étrangères des Pays-Bas. Ce manuel est destiné à servir de référence aux professionnels travaillant dans un centre de réhabilitation des personnes torturées afin de former d'autres personnes à la gestion responsable des données. Il fournit une introduction et des exercices pratiques dans le domaine de la gestion responsable et éthique des données dans le contexte de la lutte contre la torture et des droits de l'homme. Il peut être utilisé comme un outil autonome ou en conjonction avec d'autres ressources relatives à la gestion responsable des données.

Ce document a été rédigé par Carrie Gaston.

1. Introduction

L'information est un élément central de toute organisation et l'un de ses actifs les plus précieux. La gouvernance de l'information et les techniques responsables de traitement des données fournissent un cadre au traitement de cette information. Il s'agit surtout du traitement sécurisé, confidentiel et conscient des informations relatives à des **personnes identifiables** et des **informations confidentielles**.

Toute personne qui travaille pour une organisation ou au nom de celle-ci doit être consciente des éléments suivants :

- L'importance des informations détenues qui peuvent être confidentielles ou sensibles et qui concernent les utilisateurs de vos services, votre personnel, vos bénévoles, les donateurs/bailleurs de fonds ou toute autre personne associée à votre organisation.
- La législation pertinente des pays dans lesquels vous opérez, ainsi que des conseils pertinents et les meilleures pratiques pour traiter des informations de cette importance.
- Pourquoi VOUS devez assumer la responsabilité de la façon dont vous obtenez, enregistrez, utilisez, conservez et partagez l'information.
- L'impact de la gestion responsable des données sur la continuité des opérations et la capacité de continuer à fournir un service sûr et fiable à ceux que vous soutenez.

La gestion responsable des données est la responsabilité de chacun !

2. Données : Identifier les différents types de données

Dans cette section, vous enseignerez différents types et catégories de données aux participants, comment les identifier, ainsi que les risques et les mesures de protection associés à chacune d'entre elles.

Objectifs d'apprentissage - à la fin de cette section, vos participants seront à même :

- *D'identifier différentes catégories de données.*
- *De comprendre les risques possibles associés aux différentes catégories de données.*
- *De réfléchir à la manière d'appliquer des garanties à différents types de données dans leur propre contexte.*
- *D'avoir une compréhension de l'anonymisation des données à caractère personnel.*

Types de données

Dans chaque contexte organisationnel, mais plus particulièrement dans tout type d'organisation traitant de la santé et de l'aide sociale, nous sommes en contact avec différents types d'informations personnelles sur les individus.

Il est important de pouvoir identifier ces différents types d'informations afin qu'elles puissent être protégées de manière appropriée lorsqu'elles sont utilisées et partagées.

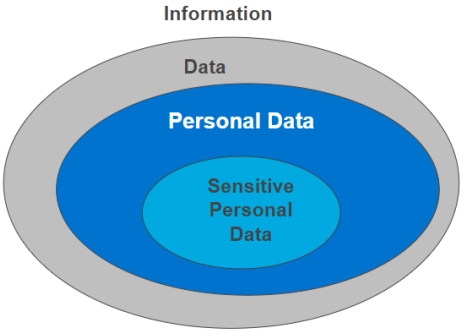
L'information est tout ensemble de faits fournis ou appris sur quelque chose.

Les données sont un ensemble de valeurs de variables qualitatives ou quantitatives.

Les données à caractère personnel (DP) sont des données relatives à une personne vivante qui peut être identifiée :

- à partir de ces données ;
- à partir de ces données et d'autres informations qui sont en possession de la personne ou de l'organisation (« responsable du traitement » dans la terminologie de la protection des données).

Les données à caractère personnel sensibles (DPS) sont une catégorie spéciale de données à caractère personnel relatives à l'origine raciale ou ethnique, aux opinions politiques, aux croyances religieuses ou similaires, à l'appartenance syndicale, à l'état de santé physique ou mentale, à la vie sexuelle, à la perpétration ou à la perpétration présumée d'un délit, quel qu'il soit.



Les informations ***confidentielles*** sont celles où il existe des aspects sensibles concernant le traitement et la divulgation de l'information. Elles peuvent être de nature personnelle ou organisationnelle. Les *données à caractère personnel sensibles* doivent généralement toujours être traitées de manière confidentielle, mais toutes les informations confidentielles ne sont pas de nature sensible ou personnelle. Par exemple, les informations stratégiques d'une entreprise peuvent entrer dans cette catégorie.

Outre le fait de réfléchir à la manière dont vous et votre organisation pouvez *protéger* les données d'une violation externe à votre organisation, il est également utile de réfléchir à la manière de mettre en œuvre de bonnes pratiques dans le traitement confidentiel des données, tant à l'extérieur qu'*à l'intérieur* de votre organisation. Cela peut signifier qu'en parallèle à cette formation, vous pensiez à mettre en œuvre des politiques et des procédures organisationnelles qui donnent à votre personnel des conseils sur les bonnes pratiques de traitement de tout élément pouvant être considéré comme confidentiel. Cela pourrait également consister en l'élaboration d'une Politique de confidentialité ou d'un Code de conduite pour le personnel.

Demandez aux participants de penser à des types d'informations dans leur contexte propre qui peuvent entrer dans cette catégorie. Demandez aux participants de dresser la liste de ces informations sur une feuille de papier et de réfléchir aux mesures de protection qu'ils peuvent avoir mises en place pour identifier et protéger cette catégorie d'informations. Une fois qu'ils ont terminé, discutez des exemples qu'ils ont notés.

Ce qui suit est un exercice de catégorisation des données. L'exercice devrait susciter une discussion sur les données personnelles et sensibles, afin de renforcer la compréhension des différentes définitions par les participants. Dans la mesure du possible, répétez l'exercice avec des versions physiques réelles de diverses données utilisées dans le contexte local. À la fin de l'exercice, les participants devraient être en mesure de :

-faire la distinction entre les données à caractère personnel, les données à caractère personnel sensibles et les données à caractère non personnel et non sensible.

Exercice 1 : Compréhension des différents types de données

Voici quelques exemples de différentes données et informations. Demandez aux participants de les placer dans la catégorie appropriée : sensibles, personnelles, ni l'une ni l'autre. La liste fournie est intentionnellement vague, afin que les participants soient encouragés à poser des questions appropriées sur les données fournies et d'avoir le sentiment de disposer de toutes les informations nécessaires pour qualifier l'élément de personnel ou de sensible. Dites-leur de réfléchir à la question de savoir si les éléments qui ne sont ni personnels ni sensibles doivent encore être traités comme étant de nature 'confidentielle '. *Demandez-leur également de réfléchir à la question de savoir s'ils ont besoin de plus d'informations pour déterminer la catégorie appropriée et noter vos questions.*

Données à caractère personnel sensibles	**Données à caractère personnel**	**Données (ni DP ni DPS)**

Les détails de la carte de crédit d'une liste des donateurs récents.	Une liste contenant des informations sur la santé mentale des patients d'une clinique	Les noms et adresses des clients

Document contenant les 10 principales langues de votre portefeuille de clients et le nombre de locuteurs de chaque langue.	La liste des clients et leur affiliation politique, en n'utilisant pas de noms, mais des numéros d'identification	Les données démographiques cumulées de tous les clients qui ont fréquenté le centre au cours de la dernière année.
Une liste des 350 clients qui se sont présentés au cours de la dernière année, ainsi que leur origine ethnique et leur orientation sexuelle.	Les résultats d'un sondage anonyme	Une liste des adresses électroniques des clients qui assistent à un groupe le vendredi.
Des informations sur les résultats d'une population de clients, p. ex. leurs notes et les variations des notes d'une mesure standard de la santé mentale	Des photocopies de passeports individuels	Des renseignements sur les postes de police et les centres de détention nommés où les clients vous ont informés avoir été détenus.
Des statistiques sur les cinq principales méthodes de torture et de traitement inhumain dont votre clientèle vous a parlé depuis l'ouverture de votre centre il y a cinq ans.	Une liste de toutes les religions auxquelles vos clients sont fidèles.	Un rapport interne contenant des renseignements commerciaux de nature sensible

Pourquoi est-il important de protéger les renseignements personnels ? Il est important de se conformer aux lois et aux meilleures pratiques afin de protéger les informations personnelles, car les informations personnelles et les informations sensibles sont précieuses. Un mauvais traitement et une mauvaise protection des données peuvent causer des dommages personnels, sociaux et réputationnels. Dans notre propre contexte de réhabilitation suite à la torture, les risques peuvent être encore plus grands et impliquer la sécurité personnelle des personnes qui accèdent à nos services.

Les moyens les plus courants de perdre des informations :

- Perte d'informations (y compris les dossiers papier) par téléphone, par télécopieur, perte d'ordinateurs ou d'appareils mobiles.

- Le vol d'informations, y compris par le biais d'attaques par hameçonnage (voir Glossaire).
- Entreposage et élimination non sécurisés des informations entraînant la perte ou le vol.

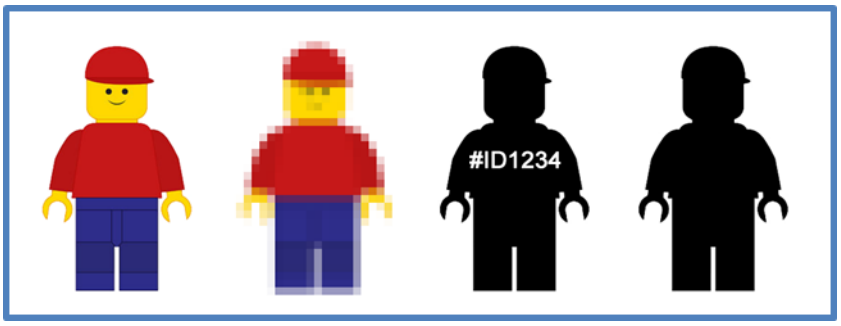
L'erreur humaine est plus dommageable que les cyberattaques

Entre octobre et décembre 2017, l'erreur humaine a représenté près des deux tiers des incidents signalés à l'Information Commissioner's Office (ICO) du Royaume-Uni, l'organisme indépendant créé pour défendre les droits à l'information. L'erreur humaine a causé plus de pertes ou de dommages que les pages Web non sécurisées et le piratage réunis, qui ne représentent que 9 %. Malgré cela, l'attention et les ressources du marché continuent de se concentrer sur les menaces externes, en particulier les cyberattaques et les pirates informatiques.

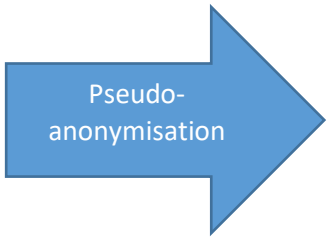
- Le classement par l'ICO des types de violations causées par l'erreur humaine révèle que les causes principales sont les suivantes :
  - Données adressées par courrier électronique au mauvais destinataire (15,8 %).
  - Perte et le vol de documents (13,1 %)
  - Données postées ou faxées au mauvais destinataire (13,0 %).

- Parmi les autres causes, mentionnons l'élimination non sécurisée du matériel et de la paperasserie, la perte ou le vol de dispositifs non chiffrés et le fait que les données n'ont pas été expurgées.

Retirer le « caractère personnel » des « données à caractère personnel » : anonymisation & pseudo-anonymisation



La **pseudo-anonymisation** est une procédure par laquelle les champs les plus caractéristiques d'un enregistrement de données sont remplacés par un ou plusieurs identificateurs artificiels, ou par des pseudonymes. Il peut y avoir un seul pseudonyme pour une série de champs remplacés ou un pseudonyme par champ remplacé. Cela permet de dissimuler l'identité réelle d'un individu, ***mais*** ce n'est pas une véritable anonymisation, car l'identité peut être facilement découverte grâce à la clé de codage utilisée.

Nom : Alisha Santos Date de naissance 21 avril 1980 Éducation : Licence en psychologie, Université de Guelph Lieu de naissance : Niagara Falls, Ontario, Canada Emploi actuel : Professeur de mathématiques à l'Université de Cambridge État civil : mariée à Dean O'Donnell Nombre d'enfants : 3.		Carte d'identité n° 357986 Date de naissance 21/04/1980 Éducation (niveau le plus élevé) : 4. Lieu de naissance : Niagara Falls, Ontario, Canada Emploi actuel : Professeur État civil : Mariée Enfants : Oui

L'**anonymisation** est le processus consistant à transformer les données en une forme qui n'identifie pas les individus et où il est peu probable que l'identification ait lieu. Cela permet une utilisation beaucoup plus large de l'information.

« Nous utilisons le terme « données anonymisées » pour désigner des données qui n'identifient pas elles-mêmes un individu et qui sont peu susceptibles de permettre l'identification d'un individu par leur combinaison avec d'autres données" (code de pratique de l'ICO sur l'anonymisation, p. 6).

Nom : Alisha Santos Date de naissance : 21 avril 1980 Éducation : Licence en psychologie, Université de Guelph Lieu de naissance : Niagara Falls, Ontario, Canada Emploi actuel : Professeur de mathématiques à l'Université de Cambridge État civil : Mariée à Dean O'Donnell Nombre d'enfants : 3.		Numéro d'identité : 357986. Tranche d'âge : 30-40 Éducation (niveau le plus élevé) : Diplôme Lieu de Naissance : Sud de l'Ontario, Canada Emploi actuel : professeur État civil : Mariée Enfants : oui

Quelques mots à propos de l'agrégation…

L'**agrégation de données** est tout processus par lequel l'information est recueillie et exprimée sous forme de résumé, par exemple à des fins d'analyse statistique. Tant que vos données ne sont pas **personnellement identifiables**, elles ne sont plus soumises aux mêmes protections législatives, bien qu'elles puissent continuer à être sensibles sur le plan commercial et donc avoir besoin d'être protégées (voir aussi *informations confidentielles* ci-dessus).

L'exercice suivant aidera les participants à réfléchir à la façon dont leurs propres données, dans leur cadre spécifique, se rapportent aux catégories de données évoquées ci-dessus. La partie (b) de l'exercice aidera les participants à réfléchir à la manière dont ils peuvent protéger certaines catégories de données, par exemple en utilisant des techniques d'anonymisation. À la fin de l'exercice, vos participants devraient être en mesure de :

-Répertorier les données dans leur propre contexte.

-Identifier ces ensembles de données en tant que données à caractère personnel ou non.

-Débattre sur les données que leur organisation peut détenir, qui ne sont pas des données à caractère personnel, mais qui doivent être traitées de manière confidentielle.

-Commencer à réfléchir à l'application de mesures de protection à différents types de données.

-Réfléchir à la façon d'appliquer l'anonymisation des données à caractère personnel avant de les partager.

-Éventuellement commencer à réfléchir à des accords de partage de données.

Exercice 2 : Compréhension des différents types de données dans votre propre contexte

(a) Dressez la liste des données communes que vous traitez (collecte, traitement, rapport, entreposage, etc.) et essayez de les classer dans les différentes catégories susmentionnées (données à caractère personnel (DP), données à caractère personnel sensibles (DPS), ni l'une ni l'autre). Certaines de ces données sont-elles potentiellement « confidentielles », mais n'entrent pas dans la catégorie « personnelles » ? Les risques associés à ces données sont-ils différents ? Appliqueriez-vous les mêmes mesures de protection à ce type de données ?

b) Pensez à des données avec lequel vous travaillez (par exemple, une liste de clients) et qu'il peut être nécessaire de partager. Pouvez-vous imaginer comment vous pourriez protéger ces informations autant que possible avant de les partager ?

3. La protection des données dans la législation (UE)

Dans cette section, vous présenterez le cadre législatif relatif à la protection des données. Cette législation récemment mise à jour n'est applicable que dans l'Union européenne, mais il est utile d'en apprendre davantage sur la norme d'excellence en matière de protection des données à plusieurs égards. Elle est également utile en tant qu'outil d'apprentissage des bonnes pratiques, même si la législation ne s'applique pas directement dans votre région du monde.

Objectifs d'apprentissage - d'ici la fin de cette section, les participants :

- *Disposeront d'une compréhension de la législation actuelle régissant la protection des données dans toute l'Union européenne.*
- *Comprendront les droits individuels des personnes concernées et les devoirs des contrôleurs et des processeurs des données.*
- *Penseront à la façon d'appliquer ces droits et ces devoirs à leurs propres données dans leur cadre respectif.*

- *Comprendront comment réaliser un exercice de cartographie des données pour identifier quelles données sont détenues et où.*
- *Comprendront ce qu'est une demande d'accès aux données (SAR en anglais) et comment s'y conformer, y compris l'expurgation de données.*

Le cadre législatif européen : Introduction au Règlement général sur la protection des données (RGPD)

Le Règlement général sur la protection des données (RGPD) de l'UE est une nouvelle législation qui prévoit une loi unique sur la protection des données à caractère personnel pour l'Union européenne. Il s'appuie sur la législation existante en matière de protection des données et la renforce dans les domaines clés suivants :

Définitions

- Une « personne concernée » est toute personne dont les données à caractère personnel sont traitées par votre organisation.
- Un « contrôleur des données » est l'entité qui détermine les finalités, les conditions et les moyens du traitement des données à caractère personnel.
- Un « processeur de données »" est l'entité qui traite les données pour le compte du contrôleur de données.

➔ ***Droits individuels*** - dans le cadre du RGPD, les droits de la personne concernée sont renforcés ou améliorés dans un certain nombre de domaines. Parmi ceux-ci :

- **Le droit à l'information** – les personnes concernées ont le droit de savoir qui fait quoi avec leurs données.
- **Le droit à l'accès -** les personnes concernées ont le droit d'avoir accès aux données personnelles que vous détenez à leur propos - cela comprend la remise d'une copie de leurs données à titre gratuit et dans un délai raisonnable (*voir aussi ci-dessous à propos des demandes d'accès aux données*).
- **Le droit de rectification -** les personnes concernées peuvent exiger la modification des données que vous détenez à leur sujet lorsqu'elles estiment qu'elles sont fausses, obsolètes ou incomplètes.
- **Le droit à l'effacement -** les personnes concernées ont désormais le droit d'exiger que leurs informations soient effacées - c'est ce qu'on appelle aussi le « droit à l'oubli ».

- **Le droit de limitation du traitement -** les personnes concernées peuvent demander le blocage ou la suppression du traitement de leurs données à caractère personnel. Dans ces circonstances, il peut être exigé que les processeurs des données continuent à entreposer les données relatives à la personne concernée afin d'étayer cette demande. (Par exemple lorsqu'un donateur ou un sympathisant a demandé à une organisation de ne plus prendre contact avec lui pour lui demander un soutien financier. Les données alors détenues constitueraient la valeur minimale à l'appui de la demande de ne plus être contacté).
- **Le droit à la portabilité des données -** permettre aux personnes concernées d'obtenir, de déplacer, de réutiliser les données d'un service à l'autre ou pour leurs propres besoins.
- **Le droit d'opposition -** les personnes concernées ont le droit de s'opposer au traitement de leurs données, y compris à des fins de marketing ou de définition de profils.
- **Les droits liés à la prise de décision automatisée, y compris la définition de profils -** il existe des exigences spécifiques afin d'être compatible avec la législation relative à la prise de décision automatisée.

➔ Le RGPD renforce ou étend la ***responsabilité des contrôleurs de données***, lorsqu'ils sont censés mettre en place des mesures globales de gouvernance et promouvoir la responsabilité et la transparence.

➔ Cela inclut également des obligations plus larges pour assurer la ***conformité des processeurs de données***, y compris les sous-traitants.

➔ Ceci comprend également des ***obligations concernant le signalement des violations de données*** et la désignation d'une personne responsable (délégué à la protection des données) dans les grandes organisations, les organismes publics et ceux qui effectuent des traitements de données à caractère personnel à grande échelle.

➔ Protection des données lors de la conception et/ou par défaut – il convient de réfléchir à la mise en œuvre de mesures de protection des données lors de la conception de tout nouveau système avant la collecte des données.

➔ Évaluations des incidences sur la vie privée - il est dûment tenu compte de toute incidence possible sur la vie privée des personnes lors de toutes les activités de traitement.

Un mot sur les demandes d'accès aux données...

En vertu de la législation actuelle et de celle proposée en matière de protection des données, toute *personne concernée* a le droit de demander les données à caractère personnel la concernant détenues par quelque organisation que ce soit. Cela signifie que toute personne peut demander une copie ou consulter les informations qu'un processeur ou un contrôleur de données détient sur elle et qu'il ne peut être refusé de se conformer à la demande. Pour répondre à une telle demande, il est important de respecter les principes (droits individuels) des personnes concernées - qui peuvent expurger certaines informations lorsque ces informations sont recueillies auprès de sources tierces, mais font partie du dossier que vous détenez.

Demandez aux participants de réfléchir à la façon dont ils répondraient à une demande d'accès aux données de la part d'une personne qui utilise leurs services. De quoi devraient-ils tenir compte pour se conformer à une telle demande ? Ont-ils pensé à des exemples où un enregistrement peut contenir des informations qui doivent être expurgées avant de se conformer à une demande ? Discutez-en en groupe.

Cartographie des données

Afin de protéger correctement les données et de vous conformer aux points ci-dessus, vous devez avant tout savoir quelles données vous détenez et où elles se trouvent. Il est judicieux d'effectuer un exercice de cartographie des données, afin que vous et les membres de votre organisation sachiez clairement quelles données sont conservées, où elles sont entreposées, combien de temps elles sont conservées, et quand et comment elles sont détruites.

Points à considérer...

De QUELLES données à caractère personnel disposez-vous ? Afin de répondre à cette question, vous devrez procéder à un examen et à une évaluation complète de TOUTES les données à caractère personnel que vous recueillez, p. ex :

- Avez-vous des informations écrites sur des bouts de papier dans un tiroir de votre bureau ?
- Avez-vous des informations personnelles inscrites dans un agenda papier ?
- Êtes-vous en mesure de vous conformer à une demande d'accès aux données (SAR en anglais) ?

OÙ sont-elles conservées ?

- Dans une base de données ?
- Sur des disques partagés/réseau ? Qui y a accès ?
- Dans des agendas papier ? Sur des bouts de papier dans votre bureau ?
- Chez vous ? Dans des courriers électroniques ?

OÙ sont-elles envoyées ?

- Pouvez-vous confirmer que vous n'envoyez des informations sur vos clients qu'à l'intérieur de votre propre pays ?
- Avez-vous l'autorisation expresse, écrite ou documentée d'envoyer les données ? Pouvez-vous le prouver ?

COMMENT sont-elles traitées ?

- Sur des ordinateurs ?
- Sur des morceaux de papier ?
- Comment protégez-vous les données en transit ?

QUE dites-vous aux personnes/aux personnes concernées au sujet du traitement des données ?

- Disposez-vous d'informations librement disponibles pour les personnes concernées ?
- Identifiez-vous les processeurs de données tiers ?
- Les données traversent-elles des frontières nationales/internationales ?

Garantie de protection des informations cliniques : S'agit-il d'informations correctes ? Sont-elles précises ? Faites-vous des contrôles et des mises à jour régulièrement ? Y a-t-il des preuves ?

L'exercice suivant aidera les participants à réfléchir de façon exhaustive aux données qu'ils recueillent et détiennent, ainsi que sur la façon et l'endroit où elles sont conservées. Ceci les aidera à savoir quelles données peuvent avoir besoin d'être protégées, mais aussi quelles sortes de protections doivent être mises en place en ce qui concerne les différents types de données. Les lacunes éventuelles dans la gestion appropriée des données seront également mises en évidence. À la fin de l'exercice, les participants devront :

-Avoir une perception des différents lieux où se trouvent les données et des formes sous lesquelles elles sont conservées.

-Réfléchir à l'endroit et à la manière dont elles sont conservées, et qui y a accès.

-Réfléchir à quel point les éléments susmentionnés sont importants pour le droit d'effacement ou pour répondre à une demande d'accès aux données.

-Commencer à penser aux calendriers de conservation des données.

Exercice 3 : Cartographie des données

Sélectionnez des données pertinentes pour votre centre (p. ex. des renseignements sur les clients) et effectuez l'exercice de cartographie des données ci-dessous en répondant aux questions suivantes :

- *Quelles sont les données recueillies ?*
- *Le consentement est-il obtenu au point de collecte ?*
- *Où sont conservées les informations ? Dans une base de données, un dossier papier, un dossier informatique ?*
- *À quelles fins servent les données ?*
- *Qui y a accès ?*
- *Arrive-t-il qu'elles soient partagées en externe ?*
- *Comment et quand les données sont-elles analysées, ajoutées ou mises à jour ?*
- *Combien de temps sont-elles conservées ?*
- *Quand et comment sont-elles effacées ?*

Apprendre des autres : Les atteintes à la protection des données dans l'actualité…

L'organisme de bienfaisance national en charge de la maladie d'Alzheimer a constaté de graves lacunes dans la façon dont il traitait les données à caractère personnel sensibles, notamment en découvrant que les bénévoles utilisaient des adresses électroniques personnelles pour recevoir et partager des informations sur les personnes qui utilisent l'organisme de bienfaisance, conservant des données non chiffrées sur leur ordinateur personnel et ne gardant pas les dossiers papier sous clé. (ICO, 07/01/2017).

Une clinique de santé condamnée à une amende de 180.000 £ (204.000 EUR, 253.000 USD) pour violation de données suite à l'envoi accidentel d'un bulletin d'information avec les adresses électroniques des destinataires dans le champ « À… »,

au lieu du champ « CCi… », révélant ainsi la séropositivité des destinataires. (ICO, 09/05/2016).

La clé USB trouvée dans l'ouest de Londres contenait des données sur la sécurité de l'aéroport (Register, 30/10/2017).

Des informations personnelles sur des enfants adoptés, des parents et des travailleurs sociaux accidentellement envoyés par courrier électronique aux invités d'une fête (Chronical Live, 26/12/2017).

Un classeur rempli de documents confidentiels du gouvernement se retrouve dans un magasin d'occasion. (Guardian, 02/02/2018).

Confidentialité : À faire et à ne pas faire

À faire

- **Protégez** la confidentialité de toutes les informations personnelles identifiables ou confidentielles avec lesquelles vous êtes en contact.
- **Soyez conscient** que toute information enregistrée au sujet d'une personne doit être protégée - cela inclut les notes et les agendas.
- **Rangez** votre bureau à la fin de chaque journée, en conservant tous les documents portables contenant des informations identifiables ou confidentielles dans des lieux d'archivage et d'entreposage identifiés, verrouillés lorsque l'accès n'est pas directement contrôlé ou supervisé.
- **Éteignez** les ordinateurs ayant accès à des renseignements personnels ou commerciaux confidentiels, ou mettez-les en mode protégé par mot de passe, si vous quittez votre bureau, quelle qu'en soit la durée.
- **Assurez-vous** de ne pouvoir être entendu lorsque vous discutez de sujets confidentiels.
- **Demandez** et **vérifiez**, au besoin, l'identité de toute personne qui fait une demande d'informations personnelles identifiables ou confidentielles et assurez-vous que cette information lui est indispensable.
- **Partagez** uniquement le minimum d'informations nécessaires.
- **Faites attention** lorsque vous envoyez de la correspondance par télécopieur ou par courrier électronique et, le cas échéant, conservez un reçu de livraison ou de lecture.
- **Transférez** les informations identifiables ou confidentielles en toute sécurité - par exemple en utilisant le cryptage des courriers électroniques.
- **Demandez conseil** si vous devez partager des informations personnelles identifiables sans le consentement de la personne identifiable et consignez la décision et toute mesure prise.
- **Signalez** toute violation réelle ou présumée de la confidentialité.

- **Participez** aux séances d'initiation, de formation et de sensibilisation aux questions de confidentialité.

À ne pas faire

- **Ne partagez pas** les mots de passe et ne les laissez pas traîner à la vue des autres.
- **Ne partagez pas** d'information sans le consentement de la personne à laquelle l'information se rapporte, à moins qu'il n'y ait des motifs légaux de le faire.
- **N'utilisez pas** d'informations permettant d'identifier une personne à moins que cela ne soit absolument nécessaire ; anonymisez les informations dans la mesure du possible.
- **Ne recueillez pas, ne conservez pas ou ne traitez pas** plus de renseignements que nécessaire et ne les conservez pas plus longtemps que nécessaire.
- **Ne pensez pas** que les commentaires ou les notes que vous faites resteront confidentiels ; les personnes ont le droit d'accéder aux renseignements conservés à leur sujet en faisant une demande d'accès aux données (SAR).
- **Ne laissez pas** d'informations sans surveillance sur votre bureau.
- Ne laissez **JAMAIS** des dossiers ou des informations dans la voiture, dans l'autobus ou lorsque vous travaillez à la maison, assurez-vous que les informations ne sont accessibles à personne d'autre que VOUS.

L'exercice suivant aidera les participants à réfléchir de manière critique sur les pratiques actuelles de leur propre organisation en utilisant certains problèmes communs de protection des données. Cela devrait les amener à réfléchir à toutes les façons dont eux-mêmes et leurs collègues traitent, entreposent et transfèrent des informations sensibles. Ils devraient tenir compte des différentes pratiques de travail et des risques potentiellement associés à ces pratiques pour les données. Ils doivent envisager les mesures de protection possibles afin de minimiser les risques pour les données. Vous pouvez demander aux participants d'élaborer eux-mêmes quelques scénarios, directement liés à leur propre organisation ou pratique. À la fin de l'exercice, les participants devront

-Être en mesure d'identifier les risques potentiels associés à leurs pratiques organisationnelles particulières.

- Être en mesure d'identifier les mesures de protection pour minimiser les risques qu'ils ont identifiés ci-dessus.

Exercice 4 : Ce à quoi il faut réfléchir

Pensez à ce que vous pourriez faire dans l'éventualité des scénarios suivants :

Vous êtes pressé de quitter le centre. Vous avez besoin de vos notes et documents pour commencer à travailler sur le rapport médico-légal, ce que vous avez l'intention de faire sur votre ordinateur portable lors du long voyage de retour en train.

Réfléchissez aux éléments suivants : Quels sont les risques possibles pour la protection des données ?

Comment pouvez-vous les minimiser ?

1. *Vous travaillez à la maison un soir sur un projet de rapport médico-légal que vous voulez faire réviser le lendemain. Comment pouvez-vous minimiser les risques pour la protection des données ?*
2. *Vous trouvez chez vous des copies papier de documents sensibles pour les clients. Comment allez-vous gérer cela ?*
3. *Vous vous rendez compte que vous avez accidentellement envoyé des informations sur un client à l'adresse de courrier électronique privée d'un collègue. Qu'allez-vous faire ? Qui allez-vous informer de l'erreur ?*

L'exercice suivant aidera les participants à comprendre comment se conformer à une demande d'accès aux données dans le cadre législatif sur la protection des données décrit ci-dessus. Les participants devront se rapporter à l'exercice précédent de cartographie des données (exercice 3) afin de trouver toute l'information dont ils peuvent disposer sur une personne, que ce soit sur papier ou sous forme électronique. Ils doivent également se demander si l'information qu'ils détiennent contient des renseignements provenant d'une tierce partie et comment ils pourraient s'y prendre pour expurger ces informations dans le cadre de leur intervention à une demande d'accès aux informations (SAR). Ils doivent également réfléchir aux conséquences possibles pour la personne et s'assurer qu'ils sont aussi clairs que possible à ce sujet (par exemple, l'envoi de données de santé sensibles par courrier électronique non sécurisé, etc.). À la fin de l'exercice, les participants doivent savoir : -Quelles sont les étapes à suivre pour traiter une demande d'accès aux données (SAR).

Exercice 5 : Conformité en matière de demande d'accès aux données (SAR)

Vous recevez un courrier électronique d'une personne qui prétend être l'avocat d'un client du centre et qui demande une copie des informations que vous détenez sur elle, à titre de demande d'accès aux données. Comment vous répondez-vous à la demande ? Que devez-

vous prendre en considération pour donner suite à la demande de manière appropriée et en temps utile ?

L'exercice suivant vise à amener les participants à réfléchir sur ce qui constitue une violation de la protection des données ou une violation de la confidentialité, et à essayer de voir quelle importance ils peuvent accorder à la gravité de ces violations. En émettant leur jugement de valeur, ils devront vous expliquer comment ils ont décidé qu'un incident était plus important ou plus grave qu'un autre. Vous devez aussi les amener à réfléchir à leur propre contexte et à ajouter leurs propres incidents à la liste. Lorsque des violations se produisent, comment s'assureront-ils de tirer les leçons de ces incidents (et de ne pas les répéter) ? À la fin de l'exercice, les participants devront être en mesure :

-D'identifier ce qui constitue une violation des données.

-D'identifier les degrés de gravité des différentes atteintes à la protection des données.

Exercice 6 : Classez les scénarios suivants par ordre de gravité, du plus élevé au moins élevé.

- *Vous trouvez des copies de documents laissés sur une photocopieuse au bureau - ces documents comprennent des lettres et une liste des problèmes de santé mentale et physique d'une personne.*
- *Un collègue vous dit qu'il a envoyé par courrier électronique des informations sur un client, y compris des données à caractère personnel sensibles sur la santé de ce dernier, à une adresse électronique erronée.*
- *Un collègue vous dit qu'il voyageait avec les données concernant des clients et qu'il les a accidentellement laissées dans le bus, le train ou à un endroit dont il ne se souvient pas.*
- *Un client très inquiet vient vous voir et vous dit que ses renseignements, ainsi que ceux d'un certain nombre d'autres clients, ont été trouvés en ligne. Ces informations comprennent des données sensibles relatives à la santé.*
- *Vous découvrez que votre bureau a été cambriolé dans la nuit. L'un des classeurs qui contiennent des informations sur les clients a été ouvert par effraction et il manque des dossiers.*
- *Vous découvrez qu'un collègue a envoyé par courrier électronique le rapport médical complet d'un client à un certain nombre de personnes de l'extérieur afin de l'utiliser comme exercice de formation, sans le consentement écrit du client.*

- *Un administrateur a accidentellement envoyé des informations sur un client (noms, données démographiques) à un cabinet d'avocats où des documents ont été adressés accidentellement avec un rapport médico-légal complet.*
- *Un rapport médico-légal contenant des données à caractère personnel très sensibles a été distribué aux participants à une formation sans anonymisation adéquate.*
- *Un administrateur a communiqué par téléphone des renseignements sur un client sans que les vérifications nécessaires aient été effectuées pour déterminer si la personne avait autorisé la communication de ces informations.*

4. Gestion responsable des données : Une vision d'ensemble au-delà de la simple protection des données

Jusqu'à présent, vous avez discuté de la protection des données et des types de données pertinentes dans certains cadres législatifs. Dans cette section, vous présenterez la gestion responsable des données aux participants. Ceci englobe un ensemble plus large de pensées, de comportements, de considérations qui s'appliquent à l'ensemble du cycle de vie des données, et pas seulement dans le contexte spécifique des données personnelles identifiables.

Objectifs d'apprentissage - à la fin de cette section, les participants :

- *Seront initiés à la notion de « données responsables ».*
- *Comprendront les implications plus précises des données responsables et éthiques dans la gestion globale des données.*
- *Exploreront les éventuelles conséquences résultant du non-respect de la gestion responsable des données.*

Qu'est-ce que la gestion responsable des données ?

L'obligation collective de tenir compte des conséquences involontaires de l'utilisation des données en :

1) Donnant la priorité aux droits qu'ont les personnes au consentement, à la vie privée, à la sécurité et à la propriété lors de l'utilisation des données dans le cadre du changement social et de leurs efforts de sensibilisation,

2) Mettant en œuvre des valeurs et des pratiques de transparence et d'ouverture.

En quoi consiste la gestion responsable des données ?

La gestion responsable des données consiste à traiter avec respect les données que nous recueillons et à défendre les droits des personnes dont nous recueillons les données.

Il s'agit de se montrer responsables et conscients des impacts sur les personnes dans tous les aspects de la gestion des données, y compris la **collecte**, la **manipulation**, l'**entreposage** et l'**utilisation** des données

Être responsable des données d'autres personnes depuis le point de collecte jusqu'à la publication du rapport.

Considérations relatives à la gestion responsable des données

Les éléments clés de la gestion responsable de données sont les suivants :

Dynamique du pouvoir : Les acteurs les moins puissants dans toute situation sont souvent les premiers à constater les conséquences involontaires des données recueillies à leur propos. Des processus comme la conception conjointe ou la participation de personnes d'origines diverses à la collecte ou à l'analyse des données peuvent atténuer ce risque.

Par exemple, dans les crises humanitaires, les personnes auprès desquelles les données sont recueillies détiennent beaucoup moins de pouvoir que celles qui demandent leurs données. Comment cette inégalité de pouvoir pourrait-elle affecter leur volonté de communiquer leurs données ?

Diversité et subjectivité : Le fait de se poser les questions suivantes : « Qui prend les décisions ? » « Quelles sont les perspectives manquantes ? » « Comment pouvons-nous inclure une diversité de pensée et d'approche ? » peut mettre en évidence les angles morts et les zones où il serait utile d'ajouter des voix supplémentaires.

Nous pensons que la diversité sous toutes ses formes renforce nos projets et notre approche. Nous avons vu des projets, des produits et des organisations souffrir d'un personnel ou de communautés homogènes - et souvent, les effets négatifs des données sont en premier lieu perçus et vécus par des communautés marginalisées. Nous devons inclure ces voix et fournir des moyens de s'améliorer en conséquence.

Inconnues : Nous ne pouvons pas voir l'avenir, mais nous pouvons intégrer des freins et contrepoids pour nous alerter si quelque chose d'inattendu se produit.

Souvent, « Mais nous ne savions pas » est la première chose que l'on entend lorsqu'il y a des conséquences négatives involontaires à un projet lié aux données. Il est de notre responsabilité de réfléchir à la façon dont nous pouvons intégrer des mesures de rectifications pour des conséquences non intentionnelles particulièrement importantes ou significatives.

Principe de précaution : Ce n'est pas parce que nous pouvons utiliser les données d'une certaine façon que nous devons le faire. Si nous ne pouvons pas suffisamment évaluer le risque et comprendre les dangers de la manipulation des données, nous devrions faire une pause d'une minute et réévaluer ce que nous faisons et pourquoi.

La technologie nous offre toutes sortes de possibilités. Toutes ne sont pas intelligentes, et toutes n'auront pas des effets positifs sur le monde. Si nous travaillons au changement social, notre priorité est de respecter et de protéger les droits des personnes - et cela exige que nous fassions preuve de réflexion sur nos propres actions.

Innovation réfléchie : Pour que les nouvelles idées aient les meilleures chances de succès - et pour que chacun puisse bénéficier de ces nouvelles idées et projets -, l'innovation doit être abordée avec soin et réflexion, et pas seulement avec rapidité.

L'innovation consiste à trouver des solutions meilleures et plus efficaces pour mieux répondre aux besoins. Pour ce faire, nous devons d'abord prendre le temps de réfléchir à la nature de ces besoins - peut-être par le biais de la recherche, peut-être par d'autres moyens. Ensuite, nous devons réfléchir aux solutions possibles pour répondre à ces besoins et, ce qui est crucial, avec des effets positifs (sans effets secondaires négatifs involontaires) sur les personnes que nous essayons d'assister à long terme.

Nous devons nous imposer des normes plus strictes : Dans de nombreux cas, les cadres juridiques et réglementaires n'ont pas encore rattrapé les effets réels des données et de la technologie. Comment pouvons-nous nous efforcer d'avoir des normes plus strictes et de donner l'exemple ?

Le fait de travailler au changement social et à la défense des droits signifie que nous nous tenons à un certain nombre d'idéaux. Le profit n'est pas notre objectif, ce dernier est plutôt un changement social positif. Dans de nombreuses régions du monde, les cadres réglementaires comportent des lacunes qui permettent la réalisation de projets qui, si nous y repensons, pourraient être considérés comme de l'exploitation. Chaque pays a des normes très différentes en matière de protection juridique de la vie privée - comme le futur Règlement général sur la protection des données à travers l'Union européenne.

Développer de meilleurs comportements : Il n'y a pas de modèle unique pour des données responsables. La culture, le contexte et les comportements en place modifient les implications et la façon dont les données sont utilisées.

La protection responsable des données ne constitue pas une pratique contraignante - malheureusement, il n'y a pas de liste de contrôle à respecter pour être considéré comme « responsable ». Il s'agit principalement d'élaborer des approches mieux informées pour travailler avec les données - ce qui peut inclure un examen régulier des décisions qui ont été prises, compte tenu des nouvelles informations. Il ne suffit pas que les personnes qui manipulent directement les données pratiquent une gestion responsable de celles-ci - c'est aussi une question opérationnelle à laquelle tout le monde, de la direction au personnel, doit réfléchir.

S'il s'agissait de vous et de vos données, comment aimeriez-vous qu'elles soient traitées, respectées et conservées en toute sécurité ?

Confidentialité - L'accès aux données doit être limité à ceux qui disposent de l'autorité appropriée.

***Intégrité* –** L'information doit être complète et exacte. Tous les systèmes et les équipements doivent fonctionner comme prévu.

Disponibilité **-** L'information doit être disponible et livrée à la personne adéquate, au moment adéquat, quand elle est nécessaire.

*Demandez aux participants d'envisager le scénario suivant, qui sert à mettre en évidence les problèmes liés à l'*intégrité *des données et à la* confidentialité. *À la fin de l'exercice, vos participants devraient être en mesure :*

-D'identifier les problèmes d'intégrité et de confidentialité des données.

-D'anticiper les conséquences possibles pour le client.

Exercice 7 : Intégrité et confidentialité des données

Scénario

JP est un client du centre et assiste régulièrement à des séances de thérapie psychologique en relation avec les tortures qu'il a subies lorsqu'il était détenu par la police d'État.

En raison d'une erreur de saisie de données, un administrateur appelle par erreur son numéro au travail plutôt que son numéro personnel et, comme JP est en réunion, un de ses collègues décroche le téléphone. Pensant être en ligne avec JP, l'administrateur lui demande s'il peut reporter son rendez-vous à une date ultérieure.
Comme l'administrateur divulgue l'origine de l'appel, il est immédiatement évident pour le collègue de JP qu'il reçoit une thérapie du centre, et il communique ensuite cette information à ses autres collègues.
Questions :

- *Quelles leçons peut-on tirer du scénario ci-dessus ?*

- *Quelles sont les conséquences possibles pour JP ?*

Indices :

- *Le numéro au travail se trouve là où le numéro personnel devrait se trouver.*
- *La confidentialité est violée lorsque l'administrateur communique ses renseignements personnels à quelqu'un d'autre que JP.*

5. Le cycle de vie des données

Dans cette partie, vous présenterez le cycle de vie des données aux participants et leur demanderez de réfléchir à la façon dont les éléments de traitement responsable des données s'intègrent à chaque étape. Vous demanderez aux participants de faire des exercices pratiques afin de s'exercer aux techniques de gestion responsable des données. Les participants doivent réfléchir aux différents types de risques et de menaces à prendre en compte aux différentes étapes du cycle de vie de la gestion des données.

Objectifs d'apprentissage - d'ici la fin de cette section, les utilisateurs :

- *Comprendront le cycle de vie des données et comment les considérations en matière de traitement responsable des données s'intègrent à chaque étape.*
- *Comprendront comment évaluer le risque en matière de gestion des données et effectueront une évaluation des risques en examinant les mesures de protection possibles.*
- *Comprendront comment tenir compte de la protection de la vie privée des gens lorsqu'il s'agit de la gestion des données et en quoi consiste une évaluation de leurs incidences sur la vie privée.*

Comprendre le cycle de vie de vos données

Le cycle de vie des données est l'enchaînement des étapes qu'un ensemble particulier de données traverse depuis sa génération initiale ou sa capture jusqu'à sa suppression ou son archivage définitifs. Il y a souvent six étapes ou davantage, identifiées dans le cycle de vie typique des données, couvrant la **collecte**, la **gestion**, l'**entreposage** et l'**utilisation** des données.

I. Collecte

1. Planification - essayez de réfléchir aux résultats que vous tentez d'atteindre et aux types d'informations dont vous aurez besoin pour y parvenir.
2. Évaluation du risque – posez-vous la question afin d'enrichir vos données ou y a-t-il une autre raison ?

3. Formation du personnel et des autres personnes chargées de la collecte des données - veillez à ce que le personnel comprenne et applique les techniques responsables de traitement des données.
4. Consentement – S'assurer d'un consentement éclairé lors de l'obtention et de l'utilisation de données à caractère personnel est considéré comme la règle d'or des bonnes pratiques.

II. Manipulation et III. Entreposage

5. Gestion - Comment allez-vous collecter, entreposer, utiliser, partager les données ? Comment vous assurerez-vous de l'exactitude de celles-ci ? Devez-vous mettre en place des mesures pour les examiner, nettoyer, purger régulièrement ?

IV. Utilisation

6. Utilisation - Comment utiliserez-vous ce qui a été collecté ?
7. Compte-rendu - L'une des clés de la gestion éthique des données est de s'assurer que ceux qui vous ont fait confiance en vous fournissant leurs données à caractère personnel reçoivent un compte-rendu chaque fois que cela est possible sur les résultats positifs obtenus en utilisant leurs données.
8. Conservation et destruction - Combien de temps dois-je conserver mes données ? Dois-je conserver toutes les données ou seulement certaines d'entre elles ? Puis-je les anonymiser ?

I. Collecte

Planification : Évaluations des risques, évaluations des facteurs relatifs à la vie privée, consentement éclairé, formation.

Étape 1 : Faites un **plan**. Définissez clairement l'objectif de la collecte des données. Les avantages que vous attendez de la collecte des données doivent être proportionnels aux risques. Vous devez être guidé par les intérêts et le bien-être des personnes sur lesquelles vous recueillez les données. NE recueillez PAS plus de données qu'il n'est nécessaire. Planifiez l'anonymisation dès la phase de conception chaque fois que cela est possible. Prévoyez comment vous obtiendrez un consentement éclairé avant de commencer.

Vérifiez qu'il n'y a aucune impartialité dans vos méthodes de collecte. Comment vérifierez-vous l'exactitude et la qualité de vos données ?

Étape 2 : Effectuez une **évaluation des risques**. La collecte de données peut mettre les gens en danger. Évaluez les risques et prenez des mesures pour éviter les conséquences négatives, par exemple en assurant la sécurité et la confidentialité des données.

Le risque d'atteinte à la vie privée est le risque de préjudice découlant d'une violation de la vie privée. Certains des moyens par lesquels ce risque peut survenir sont les informations personnelles :

- Inexactes, insuffisantes ou périmées ;
- Excessives ou non pertinentes ;
- Conservées trop longtemps ;
- Divulguées à des individus à qui la personne concernée ne veut pas les communiquer ;
- Utilisées d'une manière considérée comme inacceptable ou inattendue par l'intéressé ; ou
- Conservées de manière non sécurisée.

Le préjudice peut se présenter de différentes manières. Parfois, il sera tangible et quantifiable, par exemple une perte financière ou la perte d'un emploi. À d'autres moments, il sera moins bien défini, par exemple, les préjudices aux relations personnelles et au statut social découlant de la divulgation d'informations confidentielles ou sensibles.

Une évaluation de l'impact sur la vie privée tente d'évaluer et de rendre compte des impacts possibles sur la vie privée des individus lorsque les organisations traitent des données à caractère personnel.

Éléments à prendre en considération lors des évaluations des impacts sur la vie privée :

- Pour quel motif recueille-t-on des informations permettant d'identifier une personne ?
- Les personnes auprès desquelles je recueille des données manifestent-elles leur choix et leur accord pour le traitement de celles-ci ?
- Existe-t-il des politiques qui régissent l'utilisation et le traitement des informations

permettant une identification personnelle ? Ces politiques sont-elles fiables et adaptées à l'objectif envisagé ?

- Le personnel bénéficie-t-il d'un soutien et d'une formation régulière ?
- Existe-t-il une documentation claire concernant les lieux d'entreposage et de transmission de vos données ?
- Des protocoles clairs de partage de l'information sont-ils en place ?

L'exercice suivant aidera les participants à réfléchir à tous les aspects de la gestion des données avant de commencer un nouveau projet ou service. Les participants doivent choisir judicieusement un nouveau projet ou une nouvelle procédure et tenir compte de tous les aspects de la gestion responsable des données (GRD) dans leur plan. Cet exercice soulignera l'importance de réfléchir à la GRD avant de commencer tout nouveau projet, procédure ou service, afin que les principes de la GRD puissent être intégrés et communiqués dès le début.

Dès le début, les participants devront réfléchir à la fin du cycle de vie des données – ainsi qu'aux questions auxquelles ils tentent de répondre - par exemple, aux avantages et inconvénients d'un texte libre par rapport à des données catégorisées. À la fin de l'exercice, les participants devront être en mesure :

-D'identifier les pratiques de GRD tout au long du cycle de vie des données, du début à la fin.

Exercice 8 : Faites un plan

Demandez aux participants de se mettre par deux ou en petits groupes, et de concevoir un plan pour un nouveau projet ou service que leur organisation proposera. Veillez à ce qu'ils tiennent compte des éléments suivants dans leurs plans :

- *Quels sont les objectifs du projet ou du service ?*
- *Quel est le but de la collecte des données et que ferez-vous de celles-ci ?*
- *Quelles méthodes utiliserez-vous pour recueillir les données ?*
- *Comment obtiendrez-vous un consentement éclairé ?*
- *Comment envisagez-vous la formation de votre équipe ?*
- *Quels sont les risques et comment les gérerez-vous ?*
- *Sous quelle forme les données se présenteront-elles ? Catégorisées, non catégorisées, texte libre ?*

- *Sous quelle forme les données doivent-elles se présenter afin de se permettre le type d'analyse que vous souhaitez effectuer, le cas échéant ? Doivent-elles respecter d'autres données ? (p. ex. concordance de catégories ou de regroupements)*
- *Comment allez-vous traiter les réponses à des données catégorisées lorsque ces réponses n'existent pas (par exemple, lorsque quelqu'un répond « ni l'un ni l'autre » à la question « quel est votre sexe ? » et que les réponses dans votre système sont « masculin/féminin »).*
- *Quelles mesures de protection devez-vous mettre en place concernant l'accès, le transfert, l'entreposage ou le partage des données ?*
- *Pendant combien de temps allez-vous conserver et archiver les données et quand les éliminerez-vous ? Avez-vous un moyen d'anonymiser les données avant leur archivage ?*

L'exercice suivant aidera les participants à réfléchir de façon pratique à tous les risques associés aux divers types de traitement des données et à mettre en place des mesures de protection pour faire face à ces risques. À la fin de l'exercice, les participants devraient être en mesure :

-D'évaluer et de trouver un équilibre entre le risque lié à la collecte de données et les avantages de l'utilisation de ces données.

Exercice 9 : Évaluation des risques liés au traitement des données

Demandez à vos participants de remplir le tableau ci-dessous, d'évaluer les risques et d'attribuer un score de risque à chacun d'entre eux. Demandez-leur de préciser les contrôles qui existeraient déjà et d'essayer d'identifier les contrôles supplémentaires qu'ils pourraient avoir besoin de prévoir. Quelques suggestions possibles ont été insérées dans le tableau à leur intention. Ajoutez des risques supplémentaires à l'évaluation au fur et à mesure qu'ils les identifient.

Identification des risques et impact(s) potentiel(s)	Types de risques	Note du risque avant le contrôle : Probabilité x impact (min 0, max 25)	Contrôles/assurances existants	Note du risque après le contrôle : P x I	Autres actions prévues
Visualisation/accès non autorisé - perte de documents papier pendant le transfert.					
Personnel/bénévoles détenant des documents à la maison ou à l'extérieur.					
Courriers électroniques envoyés à partir d'adresses électroniques personnelles					
Documents envoyés par courrier électronique à un destinataire erroné					
Perte ou vol d'ordinateurs portables ou de clés USB					

	Données inexactes ou incomplètes					
	Données en double					

Étape 3 : **Formez** votre personnel. Assurez-vous que votre personnel est informé et comprend la protection des données et les considérations en matière de traitement responsable des données. Veillez à ce qu'il effectue des évaluations des risques. Assurez-vous qu'il sait comment obtenir un consentement éclairé. Veillez à ce qu'il soit formé aux meilleures pratiques en matière de sécurité des données.

Étape 4 : Obtenir un **consentement éclairé.** Expliquez aux personnes interrogées comment vous utiliserez leurs données et pourquoi vous en avez besoin.

- ➔ **Expliquer**. Expliquez clairement aux gens comment vous allez utiliser leurs informations personnelles et fournissez-leur des informations supplémentaires à ce sujet - par exemple, sur le site Web de votre organisation, dans un dépliant ou sur une affiche.
- ➔ **Donner le choix**. Donnez aux gens le choix quant à la façon dont leurs renseignements sont utilisés et informez-les si ce choix aura une incidence sur les services qui leur sont offerts.
- ➔ **Répondre aux attentes.** N'utilisez les informations personnelles que d'une manière dont les gens pourraient raisonnablement s'attendre.

Dans cet exercice, les participants réfléchiront à la façon dont ils peuvent recueillir le consentement éclairé dans leur propre contexte. Ils doivent réfléchir à toutes les façons dont ils utilisent les données des clients et s'assurer qu'elles figurent sur chaque formulaire de consentement. Les participants devront envisager de recueillir le consentement de personnes vulnérables qui peuvent avoir besoin d'explications de différentes façons, qui ne comprennent pas toujours parfaitement ce qu'est le consentement et qui peuvent par la suite se rétracter. À la fin de l'exercice, les participants devraient être en mesure :

-De s'assurer que leurs formulaires de consentement reflètent les façons dont leur organisation utilise (et prévoit d'utiliser) les informations relatives aux clients.

-De tenir compte des aspects liés au consentement des personnes vulnérables.

Exercice 10 : Consentement éclairé

En gardant à l'esprit vos propres services et contextes, élaborez un formulaire de consentement qui englobe les différentes utilisations des données dans votre organisation.

Assurez-vous que votre formulaire est clair, concis et qu'il reflète fidèlement les options possibles.

Vous pouvez également vous assurer que votre formulaire traite des accords communs de partage de données dans le cadre desquels votre service peut partager régulièrement des données avec d'autres services (p. ex. autres services de santé, etc.).

b) Avec un ou plusieurs partenaires, exercez-vous à remplir le formulaire de consentement et à obtenir un consentement éclairé.

II. Traitement et entreposage

Étape 5 : **Gérez vos données**

➔ S'assurer de la qualité des données : Nettoyer, protéger, améliorer.

Pensez à ce que vous devrez mettre en place pour assurer l'intégrité de vos dossiers et de vos données afin qu'elles soient « propres », sans doublon ni erreur.

Éléments de réflexion :

Quelles sont les conséquences possibles de données non nettoyées ? Pensez plus particulièrement à la gestion quotidienne d'un service (voir l'exemple ci-dessus concernant JP) ainsi que tout type d'analyse ou de prise de décision issues des données du participant. Quel genre d'information ou de conclusions tirent-ils (eux ou d'autres personnes), au sujet de ces données ? Quelles politiques ou quels processus devraient-ils mettre en place pour assurer la qualité des données ?

Dans l'exercice suivant, les participants réfléchiront à la valeur de données propres et standardisées et aux risques possibles de données de mauvaise qualité. Ils apprendront à standardiser un petit ensemble de données et la façon dont cela contribue à la propreté des données et peut réduire les erreurs d'analyse. À la fin de l'exercice, vos participants seront en mesure de :

-Nettoyer des données.

-Comprendre comment le nettoyage et la standardisation des données contribuent à l'intégrité de ces dernières.

Exercice 11 : Nettoyer/standardiser les données

Demandez aux participants d'examiner les données suivantes et de suggérer des moyens de les nettoyer ou de les normaliser.

Jane Doe	New York	Thérapie clinique	15 du 1, 1978
Ahmed Assan	N.Y	Thérapie	15 avril 1978
Georgeau Constantine	ny	clinique	15/01/1978

- ➔ Transfert - soyez prudents lorsque vous utilisez des dispositifs portables ou lorsque vous déplacez des documents papier. Cryptez les documents numériques. Limitez l'accès. Assurez-vous que les appareils sont cryptés. Soyez particulièrement vigilant lorsque vous déplacez des documents papier qui risquent d'être perdus ou volés.
- ➔ Accès - assurez-vous que l'accès est limité en fonction de la « nécessité de savoir ». Limitez l'accès aux systèmes et aux dossiers. Assurez-vous que les dossiers papier sont toujours sous clé et que l'accès en est contrôlé.
- ➔ Entreposage - assurez-vous de savoir et de comprendre où vos informations sont conservées.
- ➔ Partage - devez-vous partager la totalité de vos données ou seulement une partie de celles-ci ? Par exemple, des dossiers individuels pour un client ou des ensembles de données plus importants partagés avec un partenaire de recherche ?

Les participants apprendront à rédiger un accord basique de partage de données, en tenant compte des enjeux de protection des données et de la possible utilité du partage de celles-ci. Les participants devront examiner l'adéquation des techniques d'anonymisation dans le contexte de l'exemple qu'ils ont choisi. À la fin de l'exercice, les participants devront être en mesure de :

-Comprendre les enjeux de la protection des données lors du partage de celles-ci.

-Créer un accord simple de partage de données.

Exercice 12 : Accord de partage de données

Demandez aux participants de réfléchir aux partenaires avec lesquels ils travaillent et aux domaines dans lesquels ils peuvent avoir besoin de partager des données. Élaborez un accord fictif de partage de données à cette fin.

Les scénarios suivants ont pour but d'amener les participants à réfléchir à la manière dont ils pourraient concilier les besoins du service et les principes de protection des données. À la fin de l'exercice, les participants devront être en mesure de

-Trouver un équilibre entre les intérêts divergents en matière de gestion responsable des données.

Exercice 13 : éléments de réflexion

Comment réagiriez-vous ou conseilleriez-vous à vos collègues de réagir dans les scénarios suivants :

- *Vous recueillez les informations lors de l'admission d'un survivant et il vous demande ce qu'il adviendra de ces dernières.*
- *Vous recueillez des informations historiques d'un survivant par l'intermédiaire d'un traducteur, et bien que le survivant ait donné une réponse très longue et émotionnelle à une question, le traducteur a clairement fourni un résumé de ses propos.*
- *Une organisation partenaire souhaite réaliser un projet collaboratif, ce qui impliquerait un partage de données. À quoi devriez-vous penser ou que devez-vous mettre en place lorsque vous envisagez de le faire ?*
- *Un nouveau collègue rejoint votre organisation et vous demande quelle est votre politique concernant les clients qui acceptent ou qui refusent que leurs données soient utilisées pour certaines activités. Que lui dites-vous ?*

III. Utilisation

Étape 6 : **Utilisez** vos données ! Il peut s'agir de lobbying, de conscientisation ou d'apprentissage appliqué à vos propres services. Pensez à qui est représenté dans les données. Avez-vous envisagé la possibilité d'une subjectivité ? À la parité hommes-femmes ? Avez-vous confiance en la qualité des données ? Et en la qualité de l'analyse ?

Étape 7 : Fournir un **compte-rendu :** Il est recommandé d'impliquer les personnes auprès desquelles vous recueillez des données dans l'utilisation de ces dernières. Si par exemple vous avez utilisé vos données dans la rédaction d'un rapport à des fins de conscientisation, il est conseillé de partager, dans la mesure du possible, ce rapport avec les personnes interrogées.

Étape 8 : **Conservation et destruction.** Assurez-vous de disposer de politiques de conservation et de destruction appropriées. Devez-vous conserver les données sous leur forme actuelle ? Devez-vous conserver des données à caractère personnel ? Existe-t-il un moyen de ne conserver que des données agrégées ? Ou de les rendre anonymes ? Si ce n'est pas le cas, êtes-vous en mesure de récupérer des documents individuels à détruire (voir « Droit d'effacement » ci-dessus, sous RGPD) ? Lorsque vous choisissez de les supprimer, assurez-vous que la suppression est permanente et que toutes les copies ou versions sont également supprimées.

Une gestion efficace et responsable des données s'étend sur tout le cycle de vie des données.

Conclusion : par où commencer ? Ce que vous pouvez commencer à faire dès maintenant

- Sensibilisez vos collègues, sous-traitants et partenaires à la sécurité du traitement des données - en particulier les plus hauts responsables de votre organisation.
- Formez votre personnel et communiquez avec lui sur la gestion responsable des données et les mesures de sécurité des données, y compris sur les politiques visant à garantir que l'accès est protégé lorsque le personnel quitte votre organisation.
- Assurez-vous d'avoir des politiques et des procédures rigoureuses concernant la manipulation et la protection sécurisées des données à caractère personnel. Politiques : protection des données, sécurité de l'information, confidentialité, partage des données, signalement des incidents (violation), récupération, divulgation.
- Veillez à ce que les responsabilités soient clairement définies lorsqu'il s'agit de traiter les données.
- Veillez à la transparence dans la gestion des données et assurez-vous que les personnes dont vous traitez les données à caractère personnel sont clairement informées de la manière dont elles seront utilisées.
- Mettez en œuvre un système d'évaluation des risques et des incidences sur la vie privée chaque fois que vous voulez recueillir de nouvelles formes de données ou recueillir des données d'une façon différente. Un plan vous aidera

considérablement à réfléchir aux risques et aux conséquences possibles en cas d'atteinte à la protection des données.

- Utilisez une approche centrée sur le risque et réfléchissez à ce qui pourrait mal se passer afin d'essayer de mettre en place des mesures préventives pour réduire le risque.
- Obligation de franchise : soyez prêts à révéler l'existence de violations ou de pertes involontaires ou de corruption de données.
- Assurez-vous de disposer de contrats stricts pour régler les problèmes liés au partage des données ou lorsque vous sous-traitez tout type de traitement de données.
- Examinez la sécurité informatique et assurez-vous que des mesures appropriées sont en place pour le chiffrement, les sauvegardes, les mises à jour, AVEC (NDT : « Apportez Votre Équipement personnel de Communication « - équivalant de l'anglais BYOD : « Bring your own Device »), etc.
- Assurez-vous d'avoir un plan d'intervention en cas d'atteinte à la protection des données.

6. Glossaire

Agrégat - forme de regroupement dans une classe ou une concentration à des fins d'analyse de niveau supérieur ou d'anonymisation.

Atteinte à la protection des données - incident de sécurité au cours duquel des **données** sensibles, protégées ou confidentielles sont copiées, transmises, visualisées, volées ou utilisées par une personne non autorisée à le faire.

Conformité des données - l'intégrité d'un ensemble de données.

Nettoyage des données - processus de détection et de correction (ou d'élimination) des enregistrements corrompus ou inexacts d'un ensemble d'enregistrements, d'un tableau ou d'une base de données. Cela consiste à identifier les parties incomplètes, incorrectes, erronées ou non pertinentes des données puis à remplacer, modifier ou supprimer les données incorrectes ou approximatives.

Responsable du traitement des données - personne ou organisation qui détermine les objectifs pour lesquels les données à caractère personnel sont ou seront traitées, ainsi que la manière de les traiter.

Gouvernance des données - processus définis d'une organisation pour s'assurer de la qualité des données tout au long de leur cycle de vie.

Hygiène des données - processus collectifs menés pour assurer la qualité des données. Les données sont considérées comme « propres » si elles sont relativement exemptes d'erreurs. Les données « sales » peuvent causées par à un certain nombre de facteurs, y compris des enregistrements en double, des données incomplètes ou périmées et l'entreposage incorrect des champs d'enregistrement provenant de systèmes disparates.

Cycle de vie des données - le flux d'informations à travers un système, depuis la création et l'entreposage jusqu'à la suppression.

Processeur de données - toute personne ou organisation traitant des données à caractère personnel pour le compte du responsable du traitement.

Délégué à la protection des données - personnes chargées de veiller à ce qu'une ou plusieurs organisations respectent la législation sur la protection des données, et souvent leurs propres politiques internes en matière de protection des données.

Ensemble de données - ensemble de données connexes.

Accord de partage des données - accord ou cadre pour le partage des données qui définit la façon dont les données seront transmises, conservées et utilisées.

Standardisation des données - processus critique d'intégration des données dans un format commun qui permet la recherche collaborative, l'analyse à grande échelle et le partage d'outils et de méthodologies sophistiqués.

Personne concernée – personne qui fait l'objet de données à caractère personnel.

Cryptage - processus d'encodage de messages ou d'informations de telle sorte que seules les parties autorisées peuvent les lire. Le cryptage n'empêche pas en soi l'interception, mais empêche l'intercepteur d'accéder au contenu du message.

RGPD - Règlement général sur la protection des données - la nouvelle législation sur la protection des données des personnes concernées au sein de l'Union européenne.

Commissaire à l'information- autorité responsable de la surveillance et de l'application de la législation sur la protection des données au Royaume-Uni.

Éthique de l'information - « la branche de l'éthique qui se concentre sur la relation entre la création, l'organisation, la diffusion et l'utilisation de l'information, et les normes éthiques et les codes moraux régissant la conduite humaine dans la société ».

Gouvernance de l'information - la gestion de l'information au sein d'une organisation. La gouvernance de l'information établit un équilibre entre l'utilisation et la sécurité de l'information.

Consentement éclairé - un accord donné volontairement et librement, fondé sur une appréciation et une compréhension claires du fait, des implications et des conséquences potentielles d'une action.

Données à caractère personnel - données relatives à une personne vivante qui peut être identifiée à partir de ces données, ou à partir de ces données et d'autres informations en possession du responsable du traitement ou susceptibles d'entrer en sa possession.

Hameçonnage - tentative d'obtenir des informations sensibles telles que des noms d'utilisateur, des mots de passe ou des détails de carte de crédit (et parfois indirectement, de l'argent), souvent pour des raisons malveillantes, en se faisant passer pour une entité digne de confiance dans une communication électronique.

Traitement - collecte, modification, gestion, entreposage ou transmission d'informations à caractère personnel.

Évaluation des facteurs relatifs à la vie privée - évaluation visant à déterminer l'incidence de tout nouveau traitement sur la vie privée des personnes concernées. Un outil pour identifier et réduire les risques en matière de protection de la vie privée.

Pseudonyme - un nom fictif ou un alias.

Gestion des documents - domaine de la gestion responsable du contrôle efficace et systématique de la création, de la réception, de l'entretien, de l'utilisation et de l'élimination des documents. Cela comprend l'identification, le classement, l'entreposage, la sécurisation, la récupération, le suivi et la destruction ou la conservation permanente des documents.

Expurgation - censure ou obscurcissement d'une partie d'un texte ou d'une information à des fins juridiques, de sécurité, de protection de la vie privée ou d'anonymisation.

Données personnelles sensibles - se réfère aux données concernant :

- L'origine raciale ou ethnique.
- Les affiliations politiques.
- La religion ou les convictions similaires.
- L'appartenance syndicale.
- La santé mentale ou physique.
- La sexualité.
- Le casier judiciaire ou les poursuites.

Demande d'accès aux données (SAR) – toute demande (par écrit) d'une personne concernée afin d'accéder aux informations personnelles à son sujet détenues par une organisation.

7. Références/Ressources supplémentaires

- Commission sur la qualité des soins. *Des données sûres, des soins sûrs.* https://www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf
- Commissaire à la protection des données en Irlande. *RGPD et vous* http://gdprandyou.ie/
- DLA Piper, *Les lois sur la protection des données dans le monde.* https://www.dlapiperdataprotection.com/index.html?t=world-map&c=DK
- Règlement général sur la protection des données https://www.eugdpr.org/
- Geraghty, R. (2016). *Anonymisation et recherche sociale*. https://www.slideshare.net/ISSDA/anonymisation-and-social-research?qid=fa5a5338-8766-4b0b-9bf6-105f852d5932&v=&b=&from_search=1
- Bureau du commissaire à l'information https://ico.org.uk/
- Bureau du commissaire à l'information (2017). *Préparation à la Réglementation générale sur la protection des données (RGPD) : 12 étapes à suivre maintenant.* https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- Bureau du commissaire à l'information (2017). *Code de pratique sur l'accès aux données : Traiter les demandes de renseignements personnels provenant de particuliers* https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf
- Bureau du commissaire à l'information. Apportez Votre Équipement personnel de Communication *(AVEC)*. https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf
- ICRC. *Normes professionnelles pour le travail de protection.* https://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf
- Gardien des données nationales pour la santé et les soins (National Data Guardian for Health and Care) *Examen de la sécurité des données, du consentement et de la non-participation.* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
- NHS numérique. *Sensibilisation à la sécurité des données Niveau 1.* https://www.igt.hscic.gov.uk/
- NHS Angleterre. *Manuel sur la gestion de l'information.*
- Forum de données responsable : https://responsibledata.io/
- Service des données du Royaume-Uni. *Anonymisation*. https://www.ukdataservice.ac.uk/manage-data/legal-ethical/anonymisation

Annexe A

Modèle d'agenda de formation

Objectifs de formation : développer des compétences et des connaissances en matière de gestion responsable des données (collecte, traitement, entreposage, utilisation) et développer des compétences permettant de former d'autres personnes.

Jour 1

0900-10 : 30 (1,5 h)

Introduction à la gestion responsable des données

- Pourquoi faut-il les protéger ?
- Pensez à la façon dont vous aimeriez que vos propres données soient traitées.

Quelles données ?

- Données à caractère personnel, données sensibles
  → Exercice : Identifiez et classifiez les données à caractère personnel/sensibles/confidentiel.
- Anonymisation et pseudo-anonymisation
- Agrégation
  →Exercice : Dressez la liste des ensembles de données couramment traitées dans votre propre contexte ; classement de vos propres données ; commencez à réfléchir au partage de l'information.

10:30 : PAUSE (15')

10 h 45-12 h 30 (1,75 h)

Introduction au RGPD/cadre légal de l'UE

- RGPD : Le cadre légal de l'UE. Le contexte plus large et le cadre légal : Règlement général sur la protection des données (RGPD) de l'Europe
- Droits des personnes concernées ; obligations des responsables du traitement des données
  →Exercice : cartographie des données
  →Exercice : scénarios de protection des données et faire réfléchir les gens sur la façon dont ils réagiraient. Faire réfléchir les gens à des scénarios possibles dans leur propre contexte.

12 h 30 : DÉJEUNER (60')

13 h 30-15 h (1,5 h)

RGPD, suite

- Demande d'accès aux données – De quoi s'agit-il et comment y répondre ?
  →Exercice : Répondre aux demandes d'accès aux informations, aux renseignements de tiers, expurgation.
  →Exercice : Scénarios de protection des données

15:00 : PAUSE (15')

15 h 15-16 h 30 (1,25 h)
Poursuivez avec des exercices, en demandant aux participants de trouver des ensembles de données et des scénarios réels qui se rapportent à leur travail quotidien.
Pensez à la prise de décision basée sur le risque.

16 h 30 : Résumé de la journée et présentation des sujets du lendemain.

Jour 2

9 h-10 h 30 (1,5 h)
Récapitulatif des sujets de la veille
Présentation de la gestion responsable des données (GRD)

- Qu'est-ce que la GRD ?
- Pourquoi respecter l'éthique/la GRD ?
- Considérations relatives à la GRD
- Confidentialité, intégrité, disponibilité
  →Exercice : scénario et discussion

10:30 : Pause (15')

10 h 45-12 h 15 (1,5 h)
Le cycle de vie des données : Aperçu du cycle de vie des données

- Un cycle de vie ordinaire - étapes du cycle de vie des données et risques à différentes étapes.
- Collecte, entreposage, traitement, utilisation - les 8 étapes dans ce cadre.
- I. Collecte : Collecte responsable des données
  - Aperçu de la planification, éléments à prendre en compte lors de la planification de données ou d'un nouveau projet ou service, évaluations de l'impact sur la vie privée, consentement éclairé, s'assurer des compétences appropriées chez les responsables de la collecte de données, ensembles de données standardisés.
  - Évaluer le risque dans le cadre de la GRD - être prêt à faire face aux pires scénarios/apprendre des autres.

  →Exercice : Faites un plan : Pensez à une activité de service ou à un nouveau projet fondamental et à la façon dont vous pourriez procéder à une évaluation des incidences sur la vie privée concernant les données que vous recueillez. N'oubliez pas de penser aux différences entre les DP (données personnelles) et les DNP (données non personnelles).
  →Exercice : Effectuez une évaluation des risques
  - Formation de votre personnel
  - Consentement : éclairé, approprié, flexible. Consentement éclairé : de quoi s'agit-il, à quoi cela ressemble-t-il, quel est le but de la collecte, planifier le retrait du consentement ou le changement d'avis des personnes

  →Exercice : Concevez un formulaire de consentement qui sera présenté aux personnes qui accèdent à vos services au point de contact. Vous devrez réfléchir à la façon de

communiquer les raisons pour lesquelles vous utiliserez l'information et pourquoi vous en avez besoin.
→Exercice : Pratiquer l'obtention du consentement éclairé

12 h 15 – Résumé et présentation des sujets du jour 3

Jour 3

9 h 30-11 h (1,5 h)
Résumé des sujets traités jusqu'à présent/Questions et réponses
Le cycle de vie des données, suite

- II. Traitement et III. Entreposage
    - Gestion des données. Garantir l'intégrité, la qualité, la standardisation, la validité, la comparabilité des données ; relation avec les données éthiques. Mise en place d'une infrastructure appropriée ; accès contrôlé, entreposage sécuritaire (physique/électronique), partage/transfert sécuritaire - anonymisation, pseudo-anonymisation. Cryptage (Se reporter au jour 1 - demande d'accès aux données).

    →Exercice : Nettoyage des données
    - Gestion des données, suite

    →Exercice : Accords de partage des données
    →Exercice : Scénarios/points à considérer

11:00 : PAUSE

11 h 15-12 h 30 (1,25 h)

- IV. Utilisation responsable des données
    - Utilisation : Action informations(données : lobbying, promotions, évaluation du programme. Amélioration de la qualité. Changement. Envisager la manière dont les données peuvent être utilisées à *mauvais* escient.
      À quoi servent les données ? Comment pouvez-vous vous assurer qu'elles ne sont pas utilisées à mauvais escient ?
    - Compte-rendu : Fournir un compte-rendu quand c'est possible en bouclant la boucle et en transmettant les résultats et les analyses aux personnes concernées par les données - en leur montrant ce qui s'est passé/ce qui a été réalisé.
      →Exercice : Comment pourriez-vous fournir un compte-rendu aux personnes qui utilisent vos services à propos de l'utilisation que vous avez faite de leurs données ? (Pensez au partage de rapports, ou au partage des résultats d'un effort de lobbying - médias possibles : groupes/site web)

DÉJEUNER (60')

13 h 30-14 h 30 (1 h)

- Conservation et élimination. – politiques de conservation et processus appropriés existants. Les « données parallèles » - comprendre l'emplacement de

vos données : locale/en réseau/sur le cloud. Établir un lien entre la rétention et la demande d'accès aux données
→Exercice : Établissez un programme de conservation des différentes formes de données que vous conservez.

- Intégrer le GRD dans votre organisation
  →Exercice : élaborez un plan d'action sur la façon dont vous mettrez en pratique les compétences acquises au cours de la semaine écoulée et appliquez-les

PAUSE (15')

14 h 45-15 h 45 (1 h)

- Poursuivez la planification de l'action
- Compte-rendu au groupe sur la progression de votre plan d'action

15:45-16 h résumé, dernières questions et réponses