Outil d'auto-évaluation de la protection des données: Comprendre les menaces, les préjudices et les risques.

Lorsque vous utiliserez **l'outil d'auto-évaluation de la protection des données**, **vous devrez décrire les menaces, les préjudices et les risques potentiels lors de la collecte, l'utilisation ou le traitement de données.** Nous avons créé le présent document pour clarifier ces termes qui, dans notre quotidien, sont souvent employés indistinctement.

➡ *Un « risque » décrit la probabilité qu'une menace se concrétise et son impact.*

Menaces.

Les **menaces** correspondent à tout ce qui est susceptible de causer des préjudices, que ce soit de manière intentionnelle ou non: perte de données, partage de données avec un tiers non autorisé, collecte ou utilisation de données sans permission, etc. Vous trouverez ci-dessous différentes menaces en matière de protection des données qui figurent également dans l'outil d'auto-évaluation.

- **Collecte de données injustifiable ou excessive.** *Par exemple : collecte de données sur la situation matrimoniale des parents pour un projet sur la nutrition infantile.*

- **Utilisation inappropriée des données.**
  - Utilisation non raisonnable. *Par exemple : utilisation des données pour cibler l'aide selon la situation matrimoniale plutôt que les besoins.*
  - Utilisation non autorisée. *Par exemple : des bénéficiaires ont autorisé le personnel de Tdh à prendre des photos au moment d'inscrire leurs enfants. Ces photos sont maintenant utilisées pour une campagne de marketing sans le consentement explicite des parents ni des enfants.*
  - Stockage ou utilisation de données inexactes ou périmées. *Par exemple : certains enfants n'ont pas droit à une aide parce que leur âge a mal été saisi dans la base de données.*

- **Problèmes de sécurité.**
  - Perte de données. *Par exemple : perte d'une clé USB ou bris d'un disque dur contenant des données.*
  - Vol de données : des données perdues se retrouvent entre de mauvaises mains par accident ou des données sont copiées ou volées à des fins criminelles.
  - Accès, transfert, partage ou publication non justifiée de données. Les données se retrouvent entre les mains de personnes non autorisées. Il n'y a toutefois pas d'intention criminelle comme dans le cas de données volées. *Par exemple : des données sont envoyées par courrier électronique à des gens qui ne devraient pas y avoir accès ou un mot de passe est révélé à trop de personnes.*

Exemple :

A de nombreuses reprises au cours de la dernière année, des groupes armés ont volé des ordinateurs portables aux employés d'ONG dans notre zone d'intervention. Cette tendance devrait se poursuivre. Certaines de nos données font état d'abus commis par ces groupes armés. Comme nos portables ne sont pas cryptés, des collaborateurs dont le nom figure dans nos données pourraient être la cible de représailles, avec des conséquences potentiellement fatales. Le risque est élevé.

Menace = problème de sécurité : des groupes armés volent des données.

Dommage = des personnes mentionnées dans les données pourraient être ciblées et tuées.

Probabilité = élevée, comme c'est arrivé à plusieurs reprises par le passé et que la situation n'a pas changé.

Impact = majeur : il pourrait mener à des assassinats.

Gravité = élevée : le degré de probabilité est élevé et l'impact est majeur.

Préjudices.

Les **préjudices** correspondent à tout dégât, préjudice ou impact négatif — qu'il soit tangible, intangible ou économique — pouvant résulter de la manipulation de données, y compris toute violation des droits et libertés fondamentaux. Les préjudices peuvent toucher les personnes, les groupes de personnes et les organisations. Une seule menace peut causer plus d'un dommage. Préjudices les plus courants :

- Préjudices **tangibles** : blessures corporelles, perte de liberté de mouvement, préjudices à la personne ou aux biens et autres préjudices matériels ou corporels.

- Préjudices **psychologiques** : gêne, anxiété, traumatismes et autres préjudices psychologiques.

- Préjudices **sociaux** : discrimination, stigmatisation, perte de confiance, persécution judiciaire et autres préjudices sociaux.

- Préjudices **économiques** : pertes financières, détérioration des perspectives économiques et autres préjudices économiques.

Par exemple : être stigmatisé par ses voisins constitue une forme de dommage social. Être victime de violence physique constitue un dommage tangible. Être chassé de son village constitue une forme de dommage tangible (perte de sa demeure), économique (perte de biens et probablement de perspectives économiques) et social.

Risques.

Les **risques** se situent à la croisée des menaces et des préjudices. Ils décrivent la probabilité qu'une menace se concrétise et son impact. Dans l'outil d'auto-évaluation, on vous demandera d'évaluer la probabilité que certains risques se concrétisent et leur impact sur une échelle de 1 à 5. Vous trouverez ci-dessous des critères pour vous aider à évaluer le degré de risque. À partir de vos résultats, vous pourrez calculer la sévérité d'un risque (de faible à élevée) en multipliant ces deux valeurs. L'outil en ligne effectuera automatiquement ce calcul pour vous, mais un calcul manuel sera nécessaire pour la version papier.

Plus loin, nous vous indiquons à qui faire part du problème au sein de l'organisation selon s'il s'agit d'un risque faible, moyen ou élevé.

Probabilité.

Très peu probable = 1.

Possibilité minime de se concrétiser. Un risque de maximum 20 % au cours de l'année à venir, ou l'incident est très rarement survenu par le passé, voire jamais.

Peu probable = 2.

L'incident risque peu de se produire. Taux de probabilité entre 20 et 40 % au cours de la prochaine année.

Moyennement probable = 3.

La probabilité que l'incident survienne est de niveau moyen. Taux de probabilité entre 40 et 60 % au cours de la prochaine année, ou l'incident est survenu à quelques reprises par le passé.

Probable = 4.

L'incident se produira sans doute au cours de la prochaine année. Taux de probabilité entre 60 et 80 %. L'incident est déjà survenu à plusieurs reprises.

Très probable = 5.

L'incident devrait se produire. Taux de probabilité de 80 % et plus au cours de la prochaine année.

Impact.

Négligeable = 1.

Les personnes concernées peuvent facilement et rapidement gérer les préjudices sans grand effort.

Mineur = 2.

Pertes pouvant totaliser jusqu'à 5 % des actifs. En cas de dommage physique ou social, les personnes concernées seront en mesure de se rétablir complètement en peu de temps.

Modéré = 3.

Préjudices ou pertes pouvant totaliser jusqu'à 20 % des actifs, ou préjudices corporels nécessitant un traitement spécialisé. Le rétablissement par soi-même est possible, mais difficile et exige du temps.

Severe = 4.

Pertes pouvant totaliser jusqu'à 20 % des actifs, ou graves blessures ou préjudices au statut social qui nécessiteront des années pour s'en remettre. Un rétablissement complet pourrait ne pas être possible sans aide.

Critique = 5.

Conséquences catastrophiques pour les personnes touchées, comme la mort ou une perte de liberté à long terme. Perte de plus de 50 % des actifs, ou autres préjudices dont les personnes touchées ne

Degré de gravité *(calculé automatiquement).*

La version en ligne de l'outil calculera automatiquement le degré de gravité. Pour calculer manuellement la gravité du risque, multipliez la valeur de la possibilité à celle de l'impact. *Par exemple : « peu probable » (2) X « grave » (4) = 8 (risque moyen).*

Entre 1 et 6 = faible risque.

Le risque peut être limité en s'assurant que les membres de l'équipe et les gestionnaires de programme respectent la procédure habituelle.

Entre 8 et 12 = risque moyen.

Des mesures d'atténuation des risques concrètes et exhaustives doivent être mises en place à l'intérieur d'un certain délai. La mise en œuvre doit être supervisée par les supérieurs hiérarchiques.

Entre 15 et 25 = risque élevé.

Des mesures immédiates s'imposent. La haute direction du bureau national, du siège ou des deux doivent être informées des risques et des mesures d'atténuation.