



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SI-19

Dépersonnalisation

Juill. 2026



Intégrité des systèmes et des données

System and Information Integrity

SI-19 – Dépersonnalisation (Pb--)

Énoncés :

- a. Supprimer les éléments de renseignements personnels suivants des jeux de données : [\[Affectation : éléments de renseignements personnels définis par l'organisation\]](#)
- b. Évaluer l'efficacité de la dépersonnalisation [\[Affectation : fréquence définie par l'organisation\]](#) a
- a. Tenir compte des préjudices découlant de l'atteinte à la vie privée si les renseignements pouvant être accessibles au public permettent de réidentifier les individus

Responsable : Aucun

Discussion :

À l'occasion, des programmes peuvent utiliser des renseignements personnels, alors qu'ils sont en mesure d'atteindre leur objectif sans recourir aux identificateurs personnels. S'il est possible d'atteindre l'objectif sans identificateurs directs, l'information devrait être dépersonnalisée. Par dépersonnalisation, on entend le processus visant à supprimer l'association entre un jeu de données d'identification et le sujet des données. Ce processus a pour objectif d'éviter que les renseignements personnels d'un individu soient apparents lors d'une utilisation ou d'une divulgation. Plusieurs jeux de données contiennent des renseignements personnels qui peuvent être utilisés pour reconnaître ou trouver l'identité d'un individu, comme son nom, son numéro d'assurance sociale, sa date et son lieu de naissance, le nom de jeune fille de sa mère ou ses données biométriques. Les jeux de données peuvent également contenir de l'information qui est liée ou qui peut être liée à un individu, comme les renseignements médicaux ou financiers et l'information sur les études ou l'emploi. L'élimination (la suppression) des renseignements personnels est une méthode de dépersonnalisation qu'il convient d'envisager lorsqu'une telle information n'est pas (ou plus) nécessaire pour répondre aux exigences prévues pour les données ou devrait être supprimée des jeux de données par des personnes formées pour accomplir une telle tâche. Par exemple, si le jeu de données n'est utilisé que pour générer des statistiques agrégées, les identificateurs qui ne sont pas nécessaires à la production de ces statistiques sont supprimés. Supprimer les identificateurs renforce la protection de la vie privée, puisque l'information supprimée ne peut pas être divulguée par inadvertance ou utilisée de façon inappropriée. Il convient de considérer les possibles préjudices découlant de l'atteinte à la vie privée si certains renseignements peuvent permettre de réidentifier l'individu, même sans identificateurs directs. Les organisations peuvent être sujettes à des définitions ou à des méthodes de dépersonnalisation particulières en vertu des lois, de la réglementation ou des politiques applicables. La réidentification est un risque résiduel des données dépersonnalisées. Les attaques par réidentification peuvent varier et comprendre la combinaison de nouveaux jeux de données ou d'autres améliorations apportées à l'analyse de données. Demeurer au courant des attaques potentielles et évaluer l'efficacité de la dépersonnalisation au fil du temps permet de soutenir la gestion de ce risque résiduel. Il est recommandé de planifier des évaluations régulières, continues et périodiques du risque de réidentification en passant en revue les stratégies de diffusion et en modifiant les termes des accords d'échange de renseignements, le cas échéant, à mesure que les circonstances changent.