Norme internationale

ISO 30439

Management des ressources humaines — Traitement sécurisé des données

Human resource management — Safe handling of data

Première édition
2026-08

Numéro de référence
ISO 30439:2026(fr)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'ISO attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de propriété revendiqué à cet égard. À la date de publication du présent document, l'ISO n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété.

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 260, *Management des ressources humaines*.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Le présent document définit le traitement sécurisé des données dans le cadre du management des ressources humaines comme une approche responsable de la collecte, de la gestion, de la protection, de l'utilisation et de la suppression des informations à caractère personnel concernant les personnes rattachées au personnel d'un organisme. Cela concerne les actuels et anciens employés, sous-traitants, candidats et toute autre personne concernée, comme cela est défini dans le domaine d'application. Ces informations sensibles peuvent comprendre le nom d'une personne, ses coordonnées, ses informations d'identification officielles (telles que le numéro d'assurance nationale ou le numéro de sécurité sociale), ses données financières, son dossier médical et ses évaluations de performance. Compte tenu du volume considérable de données à caractère personnel traitées dans le cadre du management des ressources humaines, il est essentiel d'assurer leur confidentialité, leur intégrité, leur sécurité et leur utilisation appropriée afin d'instaurer un climat de confiance, de respecter les lois et réglementations en vigueur, et de protéger les droits des personnes. Le présent document a pour objet d'assurer une utilisation appropriée des données de management des ressources humaines, de protéger la vie privée, ainsi que de prévenir et de réduire autant que possible les conséquences de violations de données, tout en respectant les lois et réglementations locales applicables. Le présent document s'appuie sur des principes et des cadres reconnus en matière de confidentialité des données, de sécurité des données et de gestion des données.

Le présent document fournit des recommandations adaptées aux défis et aux enjeux spécifiques liés aux données de management des ressources humaines. Bien qu'il existe déjà des réglementations et des bonnes pratiques générales en matière de protection des données, l'importance et le caractère particulièrement sensible des données utilisées pour faciliter le management des ressources humaines nécessitent la mise en place d'une norme spécifique. Les données de management des ressources humaines impliquent directement des informations à caractère personnel et souvent hautement sensibles sur les employés. Un traitement inadéquat peut avoir de graves conséquences pour les personnes et les organismes. Ces risques accrus exigent un ensemble robuste de normes spécialement adaptées à la gestion des données de management des ressources humaines, afin d'assurer un niveau de protection plus élevé aux employés et aux organismes.

La mise en œuvre de pratiques rigoureuses et sûres en matière de traitement des données de management des ressources humaines présente des avantages considérables, notamment:

a) aider les organismes à conserver un avantage concurrentiel, dans un contexte où les clients, les partenaires et les employés considèrent la protection des données comme une priorité;

b) renforcer l'image de marque de l'employeur, instaurer une culture d'entreprise éthique et préserver la réputation de l'organisme, ce qui contribue à faciliter le recrutement, l'engagement et la fidélisation des employés;

c) promouvoir un sens moral, un sentiment de confiance et la loyauté auprès des personnes et des autres organismes;

d) instaurer un climat de confiance et de transparence au sein du personnel, en rassurant les employés et les candidats sur le fait que leurs informations à caractère personnel sont traitées de manière responsable;

e) réduire le risque de violations de données, d'incidents de sécurité et de perte de données précieuses;

f) optimiser les processus opérationnels pour améliorer les performances, et éviter ainsi les perturbations, les temps d'arrêt ou les pertes accidentelles de données;

g) contribuer au maintien de la conformité aux exigences légales et réglementaires.

Le non-respect des pratiques de traitement sécurisé des données de management des ressources humaines peut soulever des risques importants pour les personnes et les organismes, notamment les risques suivants:

— des sanctions financières et une responsabilité pénale en cas de non-respect des normes et exigences réglementaires en matière de protection des données;

— une utilisation abusive des données par les personnes, pouvant entraîner des fraudes et des vols d'identité, une atteinte à la confidentialité et à la vie privée, ainsi que des pertes financières pour les personnes et les organismes;

— la perte de clients, d'investissements ou de contrats;

— des répercussions sur l'organisme, telles qu'une augmentation du taux de rotation du personnel et une diminution de la capacité à recruter de nouveaux talents;

— un risque de discrimination et de préjugés préjudiciables en cas de gestion inefficace des données à caractère personnel;

— une perte de confiance des employés, une érosion de la culture d'entreprise et du moral du personnel, ainsi qu'une atteinte à la réputation;

— des interruptions d'activité et la mobilisation nécessaire de ressources humaines, financières et opérationnelles supplémentaires pour gérer, hiérarchiser et traiter les problèmes de confidentialité des données dans le cadre du management des ressources humaines qui découlent d'une compromission de données.

Outre les recommandations du présent document relatives au traitement sécurisé des données de management des ressources humaines, d'autres normes peuvent fournir des recommandations supplémentaires concernant la gestion et la protection générales de certains types de données de management des ressources humaines. Par exemple, la série ISO 10667 se concentre sur la méthode et la procédure systématiques permettant de confirmer ou mesurer les connaissances, le savoir-faire, les aptitudes, les performances ou d'autres caractéristiques de nature professionnelle d'une personne ou d'un groupe de personnes. Elle formule également des suggestions visant à assurer la protection des données des participants à l'évaluation et l'utilisation appropriée des données à caractère personnel.

Management des ressources humaines — Traitement sécurisé des données

1 Domaine d'application

Le présent document définit des lignes directrices à l'intention des organismes en ce qui concerne le traitement sécurisé des données de management des ressources humaines, afin d'assurer une approche responsable de la collecte, de la gestion, de la protection, de l'utilisation et de la suppression des informations à caractère personnel concernant le personnel d'un organisme. Le présent document s'applique aussi bien aux organisations à but lucratif qu'aux organisations à but non lucratif, indépendamment de leur taille et de leur secteur d'activité. Elle s'applique à tous les secteurs et à toutes les tailles d'organismes, et couvre les données des actuels et anciens employés, sous-traitants, candidats et de toute autre personne concernée. Le présent document traite des données qui sont obtenues dans le cadre des activités et processus de management des ressources humaines, qui en sont issues ou qui sont utilisées dans ce cadre.

Le présent document couvre le traitement sécurisé des données de management des ressources humaines, quel que soit leur format, qu'elles soient collectées, tenues à jour ou utilisées par un service des ressources humaines ou par une autre entité, telle que des tiers, des fournisseurs ou des services autres que celui des ressources humaines (par exemple, le service financier ou le service opérationnel). Le présent document porte exclusivement sur le traitement sécurisé des données de management des ressources humaines; les caractéristiques de ces données, telles que leur qualité, leur fiabilité et leur validité, ne relèvent pas du domaine d'application du présent document (voir l'ISO 30435). Le présent document concerne les données relatives à toute personne dont les informations sont utilisées dans le cadre du cycle de vie des données de management des ressources humaines, y compris les actuels et anciens employés, sous-traitants, dirigeants ou membres du conseil d'administration, les candidats, ainsi que les personnes anciennement ou indirectement associées à l'organisme. Il ne couvre pas la protection de la vie privée des clients, fournisseurs ou autres tiers lorsque les données se trouvent en dehors du cadre du management des ressources humaines (voir l'ISO/IEC 27001 et l'ISO/IEC 27002 pour la protection des données non spécifiques au management des ressources humaines, ainsi que la série ISO/IEC 38505 relative à la gouvernance des données en général).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 30400, *Management des ressources humaines — Vocabulaire*

ISO/IEC 27000, *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Vue d'ensemble*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO 30400, de l'ISO/IEC 27000 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1
automatisé
sans entrée ou intervention manuelle (par exemple via des moyens électroniques, tels qu'un réseau informatique)

[SOURCE: ISO/IEC 19790:2025, 3.3]

3.2
violation de données
compromission de sécurité qui entraîne la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès à des données protégées transmises, stockées, ou soumises à un quelconque autre traitement

[SOURCE: ISO/IEC 27040:2024, 3.5.2]

3.3
discrimination
situation dans laquelle une personne ou un groupe social est intentionnellement ou effectivement traité, en raison de son appartenance à un groupe, de manière moins favorable qu'une autre personne ou un autre groupe ne l'est, ne l'a été ou ne le serait dans une situation comparable

3.4
vol d'identité
résultat d'une fausse déclaration d'identité réussie

[SOURCE: ISO/IEC 24760-3:2025, 3.3]

3.5
traitement sécurisé des données
processus consistant à stocker, gérer, utiliser les données et en gérer le sort final de manière sécurisée et responsable

3.6
transparence
accessibilité des informations relatives aux décisions et aux activités ayant une incidence sur la société, l'économie et l'environnement, et volonté d'en assurer une communication claire, exacte, en temps voulu, honnête et complète

[SOURCE: ISO 26000:2010, 2.24]

4 Généralités

Compte tenu de la nature sensible des données de management des ressources humaines (notamment les identifiants personnels, les informations financières, les dossiers médicaux et les évaluations de performance), il est essentiel de traiter ces données de manière appropriée afin de préserver leur confidentialité, leur intégrité et leur conformité aux exigences légales et réglementaires. Le présent document traite des enjeux spécifiques de la sécurité des données de management des ressources humaines et souligne l'importance de mettre en place des mesures de protection solides pour atténuer les risques, tels que les violations de données, le vol d'identité, les sanctions réglementaires et l'atteinte à la réputation. Les organismes qui mettent en œuvre ces bonnes pratiques bénéficient d'une confiance accrue, d'une meilleure efficacité opérationnelle, d'une image de marque plus forte en tant qu'employeur et d'une réduction des risques juridiques et de sécurité. Bien qu'il porte spécifiquement sur les données de management des ressources humaines, le présent document est harmonisé avec les cadres plus généraux en matière de protection des données, et s'inscrit en complément des Normes internationales connexes; il peut, par exemple, être utilisé dans le cadre du cycle “planifier, appliquer, vérifier, réviser” afin d'appuyer et faciliter la mise en place d'un cadre de gestion des données sécurisé et éthique en matière de management des ressources humaines. L'utilisation de ce cadre permet d'assurer le maintien du cycle d'amélioration continue et de veiller à ce que le processus de traitement des données reste en phase avec les exigences en constante évolution de l'organisme. Il est recommandé que les organismes utilisent ce cadre et cette approche tout au

long du processus de traitement des données. Pour mieux cerner le contexte, ce cadre peut être clarifié de la manière suivante:

— Planifier: identifier et évaluer les risques et opportunités associés, puis définir les objectifs et les processus nécessaires pour obtenir des résultats, conformément aux politiques, processus et objectifs de l'organisme;

— Appliquer: mettre en œuvre les processus selon les modalités prévues;

— Vérifier: surveiller et mesurer les activités et les processus liés au traitement sécurisé des données, ainsi que les objectifs organisationnels, puis rendre compte des résultats;

— Réviser: prendre des mesures d'amélioration continue du traitement des données afin d'atteindre les résultats escomptés. Les améliorations identifiées au cours de cette étape serviront de base à l'élaboration d'un plan ultérieur, afin d'assurer la poursuite du cycle.

Ce cadre illustre un exemple de processus d'amélioration continue et peut être remplacé par un autre processus, selon ce que l'organisme jugera approprié; il est toutefois recommandé de mettre en œuvre un cadre d'amélioration continue.

5 Données de management des ressources humaines

5.1 Généralités

Le management des ressources humaines repose sur la collecte, le stockage et l'utilisation d'informations, notamment des données concernant les employés actuels, anciens ou potentiels, ainsi que des informations relatives à d'autres personnes telles que les conjoints, les personnes à charge, les proches et toute autre information nécessaire à la gestion des relations professionnelles. Les données de management des ressources humaines associées à un organisme peuvent varier et sont propres à cet organisme. Le présent document décrit les différents types de données de management des ressources humaines fréquemment rencontrés quels que soient le secteur d'activité et la taille de l'organisme, afin de fournir des exemples de traitement sécurisé des données dans le contexte du management des ressources humaines (par exemple, le 6.4.1 et le 6.4.2 s'appuient sur des exemples de types de données de management des ressources humaines pour faciliter la compréhension). D'autres exemples de données de management des ressources humaines figurent dans l'ISO 30435.

Les données de management des ressources humaines interviennent à toutes les étapes du cycle de vie du personnel (par exemple, données de recrutement, données de performance, données relatives aux départs du personnel) et ces données ont un cycle de vie qui leur est propre (par exemple, création, stockage, gestion, suppression). Pour mieux comprendre le traitement sécurisé des données de management des ressources humaines, il est donc important de l'appréhender dans le contexte de ces deux cycles de vie interconnectés: le cycle de vie du personnel (5.2) et le cycle de vie de la gestion des données (5.3).

5.2 Cycle de vie du personnel

Le cycle de vie du personnel peut apporter des éclairages sur les données qui nécessitent un traitement sécurisé et qu'un organisme collecte, stocke, utilise, partage, conserve ou dont il gère le sort final. Le cycle de vie du personnel forme un cadre qui résume les activités que mènent un organisme et une personne, et qu'ils considèrent comme pertinentes pour la gestion des effectifs. Il englobe une série d'étapes liées à l'emploi et un ensemble de processus organisationnels (tels que la planification des effectifs, la rémunération, le recrutement, l'intégration, la formation et le développement, la gestion des performances, la planification de la relève, la mobilité du personnel et la cessation d'emploi), chacune de ces étapes et chacun de ces processus étant susceptibles de générer et d'utiliser des données pertinentes dans le contexte du management des ressources humaines. Le présent document n'a pas pour objet de définir ou de recommander un modèle unique de cycle de vie du personnel, car ce cycle peut varier selon les régions, les secteurs d'activité et la taille de l'organisme. Toutefois, il convient d'envisager le traitement sécurisé des données de management des ressources humaines dans le contexte du cycle de vie du personnel afin de faciliter l'identification de l'ensemble de ces données. De plus amples informations sur le cycle de vie du personnel sont disponibles dans l'ISO 30435.