International Standard

ISO 30439

Human resource management — Safe handling of data

Management des ressources humaines — Traitement sécurisé des données

First edition
2026-08

Reference number
ISO 30439:2026(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 260, *Human resource management*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document presents safe data handling in human resource management (HRM) as the responsible collection, management, protection, usage and disposal of personal information pertaining to individuals associated with an organization's workforce. This includes current and former employees, contractors, applicants and other relevant individuals as defined in the scope. This sensitive information may encompass an individual's name, contact details, governmental identification information, such as national insurance or social security numbers, financial data, health records, performance evaluations. Given the vast amount of personal data processed within HRM, ensuring its confidentiality, integrity, security, and appropriate use is essential for building trust, maintaining compliance with laws and regulations, and safeguarding the rights of individuals. The goal of this document is to ensure the appropriate use of HRM data, protect privacy, and prevent and minimize the impact of data breaches while complying with applicable local laws and regulations. This document is informed by recognized data privacy, data security and data management principles and frameworks.

This document provides guidance tailored to the unique challenges and considerations of HRM data. While broader data privacy regulations and best practices exist, the prevalence and unique sensitivity of data used to facilitate HRM necessitates a dedicated standard. HRM data directly involves personal and often highly sensitive employee information. Improper handling can have severe consequences for individuals and organizations. These heightened risks demand a robust set of standards specifically tailored to HRM data management, ensuring a higher level of protection for employees and organizations.

There are significant advantages to implementing robust safe handling practices for HRM data. Benefits can include:

a) helping organizations maintain a competitive edge, as customers, partners and employees prioritize data protection;

b) enhancing employer brand, ethical workplace culture and organizational reputation, which supports recruitment, employee engagement and retention;

c) promoting morale, trust and loyalty with individuals and other organizations;

d) engendering trust and transparency within the workforce, reassuring employees and candidates that their personal information is handled responsibly;

e) reducing risk of data breaches, security incidents and loss of valuable data;

f) enhancing operational processes for better performance, which avoids disruptions, downtime or accidental data loss;

g) helping to maintain compliance with legal and regulatory requirements.

Failure to follow proper safe handling practices for HRM data can present significant risks for individuals and organizations, which can include but are not limited to the following:

— financial penalties and criminal liability due to non-compliance with data privacy standards and regulatory requirements;

— data misuse by individuals, which can lead to fraud and identity theft, loss of confidentiality and privacy, and monetary loss for individuals and organizations;

— losing customers, investments or contracts;

— organizational impacts such as increased employee turnover and decreased ability to recruit new talent;

— potential for discrimination and harmful bias if personal data are not managed effectively;

— losing employee trust, erosion of culture and morale and reputational damage;

— operational downtime and additional human, financial and operational resources required to manage, triage and respond to HRM data privacy issues arising from compromised data.

In addition to the safe handling recommendations for HRM data included within this document, other standards can provide additional guidance for the general management and protection of certain types of HRM data. For example, the ISO 10667 series focuses on the systematic method and procedure for ascertaining or measuring work-related knowledge, skills, abilities, performance, or other characteristics of an individual or group of individuals. It also provides suggestions for ensuring assessment participants' data protection and appropriate use of personal data.

Human resource management — Safe handling of data

1 Scope

This document establishes guidelines for organizations in the safe handling of human resource management (HRM) data, ensuring responsible collection, management, protection, usage and disposal of personal information related to an organization's workforce. This document applies to both for-profit and non-profit organizations of any size in all sectors. It applies to all sectors and organization sizes, covering data from current and former employees, contractors, applicants and other relevant individuals. This document pertains to data derived for, from, or used within HRM activities and processes.

This document covers the safe handling of HRM data, in any format, whether collected, maintained or used by a human resources department or an alternative party such as third parties, vendors or non-HR departments (e.g. finance, operations). This document concerns only the safe handling of HRM data; characteristics of the HRM data such as the quality, reliability and validity are not within the scope of this document (see ISO 30435). This document covers data related to any individual for whom information is utilized as part of the HRM data life cycle, including past and present employees, contractors, directors or board members, applicants, and formerly or indirectly associated individuals. It does not include privacy for customers, suppliers or other third parties when the data exists outside of HRM (see ISO/IEC 27001 and ISO/IEC 27002 for data privacy non-specific to HRM data and the ISO/IEC 38505 series related to data governance in general).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 30400, *Human resource management — Vocabulary*

ISO/IEC 27000, *Information security, cybersecurity and privacy protection — Information security management systems — Overview*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 30400, ISO/IEC 27000, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
automated
without manual intervention or input (e.g. electronic means such as through a computer network)

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