



DPC: 25/30469627 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 13 October 2025

Origin: International

Latest date for receipt of comments: 06 December 2025

Project No. 2023/00318

Responsible committee: HCS/1 Human Capital

Interested committees:

Title: Draft BS ISO 30439 Human Resource Management — Safe Handling of Data.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 06 December 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 30439

Human Resource Management — Safe Handling of Data

ICS: 03.100.30; 35.030

ISO/TC 260

Secretariat: **ANSI**

Voting begins on:
2025-10-13

Voting terminates on:
2026-01-05

This document has not been edited by the ISO Central Secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/DIS 30439:2025(en)

Full document details: 25/30469627 DC

© ISO 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 General	2
5 HRM data	3
5.1 Workforce life cycle	3
5.2 Data management life cycle	3
5.3 Safe handling classification of HRM data	3
5.3.1 Sensitivity-based classification	4
5.3.2 Risk-based classification	4
6 HRM safe data handling	5
6.1 Data minimization and purpose limitation	5
6.2 HRM access controls	5
6.3 HRM data collection	6
6.3.1 Notice	6
6.3.2 Consent	6
6.4 HRM data processing	7
6.4.1 Analysis and reporting	7
6.4.2 Decision-making	7
6.4.3 Data joins	8
6.5 HRM data sharing	8
6.6 HRM data storage, retention, and deletion	8
6.6.1 Storing data	8
6.6.2 Retention	9
6.6.3 Disposal and deletion	10
7 HRM safe data handling training	10
8 Communication and transparency	11
9 Governance for the safe handling of data	11
9.1 Governance materials	12
9.2 Roles and responsibilities	12
9.3 Risk assessments	13
9.4 Monitoring and auditing	14
9.4.1 Monitoring	14
9.4.2 Auditing	14
9.5 HRM data breach response	14
9.6 Integration of third parties	15
Annex A (informative) Responsibility assignment matrix (RACI) model	16
Bibliography	18

Foreword

The International Organization for Standardization (ISO) 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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 standard 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, etc. 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 standard 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 standard is informed by recognized data privacy, data security, and data management principles and frameworks.

Unique challenges and benefits of HRM data safe handling

This standard 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 the organization.

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 may include but are not limited to the following:

- a) Financial penalties and criminal liability due to non-compliance with data privacy standards and regulatory requirements.
- b) Data misuse by individuals, which may lead to fraud and identity theft, loss of confidentiality and privacy, and monetary loss for individuals and organizations.
- c) Losing customers, investments, or contracts.
- d) Organizational impacts such as increased employee turnover, decreased ability to recruit new talent, and other operational impacts.
- e) Potential for discrimination and harmful bias if personal data are not managed effectively.
- f) Losing employee trust, erosion of culture and morale, and reputational damage.

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