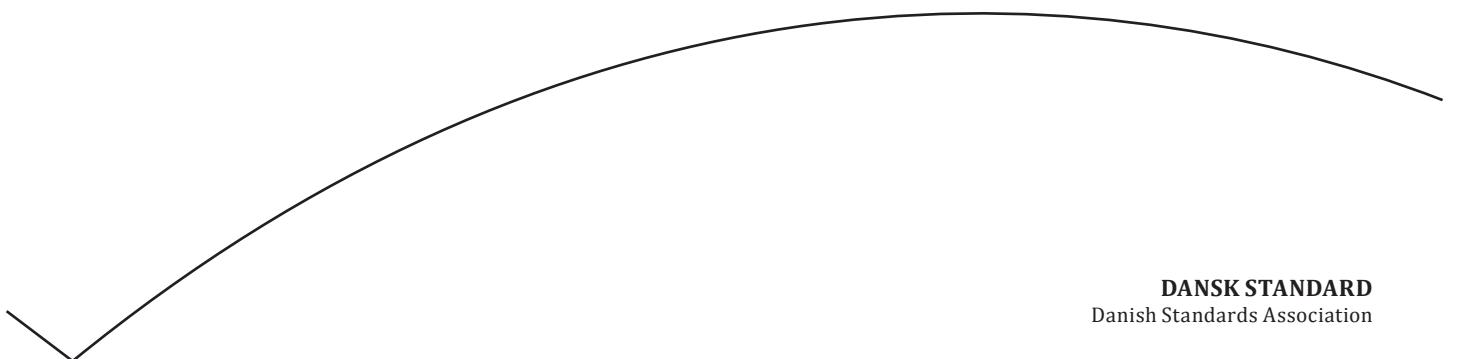




This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.

Sikkerhedsteknikker – Forlængelse til ISO/IEC 27001 og ISO/IEC 27002 med henblik på styring af personfølsomme oplysninger – Krav og retningslinjer

Security techniques – Extension to ISO/IEC
27001 and ISO/IEC 27002 for privacy information
management – Requirements and guidelines



DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn
Tel: +45 39 96 61 01
Tel: +45 39 96 61 01
dansk.standard@ds.dk
www.ds.dk

This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.

DS projekt: M328534

ICS: 35.030

Første del af denne publikations betegnelse er:

DS/ISO/IEC, hvilket betyder, at det er en international standard, der har status som dansk standard.

Denne publikations overensstemmelse er:

IDT med: ISO/IEC 27701:2019

DS-publikationen er på engelsk.

DS-publikationstyper

Dansk Standard udgiver forskellige publikationstyper.

Typen på denne publikation fremgår af forsiden.

Der kan være tale om:

Dansk standard

- standard, der er udarbejdet på nationalt niveau, eller som er baseret på et andet lands nationale standard, eller
- standard, der er udarbejdet på internationalt og/eller europæisk niveau, og som har fået status som dansk standard

DS-information

- publikation, der er udarbejdet på nationalt niveau, og som ikke har opnået status som standard, eller
- publikation, der er udarbejdet på internationalt og/eller europæisk niveau, og som ikke har fået status som standard, fx en teknisk rapport, eller
- europæisk præstandard

DS-håndbog

- samling af standarder, eventuelt suppleret med informativt materiale

DS-hæfte

- publikation med informativt materiale

Til disse publikationstyper kan endvidere udgives

- tillæg og rettelsesblade

DS-publikationsform

Publikationstyperne udgives i forskellig form som henholdsvis

- fuldtekstpublikation (publikationen er trykt i sin helhed)
- godkendelsesblad (publipukationen leveres i kopi med et trykt DS-omslag)
- elektronisk (publikationen leveres på et elektronisk medie)

DS-betegnelse

Alle DS-publikationers betegnelse begynder med DS efterfulgt af et eller flere præfikser og et nr., fx **DS 383**, **DS/EN 5414** osv. Hvis der efter nr. er angivet et **A** eller **Cor**, betyder det, enten at det er et **tillæg** eller et **rettelsesblad** til hovedstandarden, eller at det er indført i hovedstandarden.

DS-betegnelse angives på forsiden.

Overensstemmelse med anden publikation:

Overensstemmelse kan enten være IDT, EQV, NEQ eller MOD

- **IDT:** Når publikationen er identisk med en given publikation.
- **EQV:** Når publikationen teknisk er i overensstemmelse med en given publikation, men præsentationen er ændret.
- **NEQ:** Når publikationen teknisk eller præsentationsmæssigt ikke er i overensstemmelse med en given standard, men udarbejdet på baggrund af denne.
- **MOD:** Når publikationen er modifieret i forhold til en given publikation.

This is a preview of "DS/ISO/IEC 27701:201...". Click [here](#) to purchase the full version from the ANSI store.

First edition
2019-08-06

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices



Reference number
ISO/IEC 27701:2019(E)

© ISO/IEC 2019

This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.

Contents

	Page
Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviations	1
4 General	2
4.1 Structure of this document	2
4.2 Application of ISO/IEC 27001:2013 requirements	2
4.3 Application of ISO/IEC 27002:2013 guidelines	3
4.4 Customer	4
5 PIMS-specific requirements related to ISO/IEC 27001	4
5.1 General	4
5.2 Context of the organization	4
5.2.1 Understanding the organization and its context	4
5.2.2 Understanding the needs and expectations of interested parties	5
5.2.3 Determining the scope of the information security management system	5
5.2.4 Information security management system	5
5.3 Leadership	5
5.3.1 Leadership and commitment	5
5.3.2 Policy	5
5.3.3 Organizational roles, responsibilities and authorities	5
5.4 Planning	6
5.4.1 Actions to address risks and opportunities	6
5.4.2 Information security objectives and planning to achieve them	7
5.5 Support	7
5.5.1 Resources	7
5.5.2 Competence	7
5.5.3 Awareness	7
5.5.4 Communication	7
5.5.5 Documented information	7
5.6 Operation	7
5.6.1 Operational planning and control	7
5.6.2 Information security risk assessment	7
5.6.3 Information security risk treatment	8
5.7 Performance evaluation	8
5.7.1 Monitoring, measurement, analysis and evaluation	8
5.7.2 Internal audit	8
5.7.3 Management review	8
5.8 Improvement	8
5.8.1 Nonconformity and corrective action	8
5.8.2 Continual improvement	8
6 PIMS-specific guidance related to ISO/IEC 27002	8
6.1 General	8
6.2 Information security policies	8
6.2.1 Management direction for information security	8
6.3 Organization of information security	9
6.3.1 Internal organization	9
6.3.2 Mobile devices and teleworking	10
6.4 Human resource security	10
6.4.1 Prior to employment	10
6.4.2 During employment	10
6.4.3 Termination and change of employment	11

This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.

6.5	Asset management	11
6.5.1	Responsibility for assets	11
6.5.2	Information classification	11
6.5.3	Media handling	12
6.6	Access control	13
6.6.1	Business requirements of access control	13
6.6.2	User access management	13
6.6.3	User responsibilities	14
6.6.4	System and application access control	14
6.7	Cryptography	15
6.7.1	Cryptographic controls	15
6.8	Physical and environmental security	15
6.8.1	Secure areas	15
6.8.2	Equipment	16
6.9	Operations security	17
6.9.1	Operational procedures and responsibilities	17
6.9.2	Protection from malware	17
6.9.3	Backup	17
6.9.4	Logging and monitoring	18
6.9.5	Control of operational software	19
6.9.6	Technical vulnerability management	19
6.9.7	Information systems audit considerations	19
6.10	Communications security	20
6.10.1	Network security management	20
6.10.2	Information transfer	20
6.11	Systems acquisition, development and maintenance	21
6.11.1	Security requirements of information systems	21
6.11.2	Security in development and support processes	21
6.11.3	Test data	23
6.12	Supplier relationships	23
6.12.1	Information security in supplier relationships	23
6.12.2	Supplier service delivery management	24
6.13	Information security incident management	24
6.13.1	Management of information security incidents and improvements	24
6.14	Information security aspects of business continuity management	26
6.14.1	Information security continuity	26
6.14.2	Redundancies	27
6.15	Compliance	27
6.15.1	Compliance with legal and contractual requirements	27
6.15.2	Information security reviews	28
7	Additional ISO/IEC 27002 guidance for PII controllers	28
7.1	General	28
7.2	Conditions for collection and processing	28
7.2.1	Identify and document purpose	28
7.2.2	Identify lawful basis	29
7.2.3	Determine when and how consent is to be obtained	30
7.2.4	Obtain and record consent	30
7.2.5	Privacy impact assessment	30
7.2.6	Contracts with PII processors	31
7.2.7	Joint PII controller	31
7.2.8	Records related to processing PII	32
7.3	Obligations to PII principals	32
7.3.1	Determining and fulfilling obligations to PII principals	32
7.3.2	Determining information for PII principals	33
7.3.3	Providing information to PII principals	33
7.3.4	Providing mechanism to modify or withdraw consent	34
7.3.5	Providing mechanism to object to PII processing	34
7.3.6	Access, correction and/or erasure	35

This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.

7.3.7	PII controllers' obligations to inform third parties.....	35
7.3.8	Providing copy of PII processed.....	35
7.3.9	Handling requests.....	36
7.3.10	Automated decision making.....	36
7.4	Privacy by design and privacy by default.....	37
7.4.1	Limit collection.....	37
7.4.2	Limit processing.....	37
7.4.3	Accuracy and quality	37
7.4.4	PII minimization objectives.....	38
7.4.5	PII de-identification and deletion at the end of processing.....	38
7.4.6	Temporary files.....	38
7.4.7	Retention	39
7.4.8	Disposal	39
7.4.9	PII transmission controls	39
7.5	PII sharing, transfer, and disclosure	40
7.5.1	Identify basis for PII transfer between jurisdictions.....	40
7.5.2	Countries and international organizations to which PII can be transferred	40
7.5.3	Records of transfer of PII.....	40
7.5.4	Records of PII disclosure to third parties.....	41
8	Additional ISO/IEC 27002 guidance for PII processors.....	41
8.1	General.....	41
8.2	Conditions for collection and processing.....	41
8.2.1	Customer agreement.....	41
8.2.2	Organization's purposes	42
8.2.3	Marketing and advertising use	42
8.2.4	Infringing instruction	42
8.2.5	Customer obligations	42
8.2.6	Records related to processing PII.....	43
8.3	Obligations to PII principals.....	43
8.3.1	Obligations to PII principals	43
8.4	Privacy by design and privacy by default.....	44
8.4.1	Temporary files.....	44
8.4.2	Return, transfer or disposal of PII.....	44
8.4.3	PII transmission controls	44
8.5	PII sharing, transfer, and disclosure	45
8.5.1	Basis for PII transfer between jurisdictions.....	45
8.5.2	Countries and international organizations to which PII can be transferred	45
8.5.3	Records of PII disclosure to third parties.....	46
8.5.4	Notification of PII disclosure requests.....	46
8.5.5	Legally binding PII disclosures	46
8.5.6	Disclosure of subcontractors used to process PII	46
8.5.7	Engagement of a subcontractor to process PII	47
8.5.8	Change of subcontractor to process PII	47
	Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers).....	48
	Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors).....	52
	Annex C (informative) Mapping to ISO/IEC 29100.....	55
	Annex D (informative) Mapping to the General Data Protection Regulation	57
	Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151.....	60
	Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002.....	63
	Bibliography	65

This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 and IEC 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) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

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.

This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.

Introduction

0.1 General

Almost every organization processes Personally Identifiable Information (PII). Further, the quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated legislation and/or regulation all over the world.

The Information Security Management System (ISMS) defined in [ISO/IEC 27001](#) is designed to permit the addition of sector specific requirements, without the need to develop a new Management System. ISO Management System standards, including the sector specific ones, are designed to be able to be implemented either separately or as a combined Management System.

Requirements and guidance for PII protection vary depending on the context of the organization, in particular where national legislation and/or regulation exist. [ISO/IEC 27001](#) requires that this context be understood and taken into account. This document includes mapping to:

- the privacy framework and principles defined in [ISO/IEC 29100](#);
- [ISO/IEC 27018](#);
- [ISO/IEC 29151](#); and
- the EU General Data Protection Regulation.

However, these can need to be interpreted to take into account local legislation and/or regulation.

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

An organization complying with the requirements in this document will generate documentary evidence of how it handles the processing of PII. Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This can also assist in relationships with other stakeholders. The use of this document in conjunction with [ISO/IEC 27001](#) can, if desired, provide independent verification of this evidence.

This document was initially developed as [ISO/IEC 27552](#).

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its Management System Standards.

This document enables an organization to align or integrate its PIMS with the requirements of other Management System standards.

This is a preview of "DS/ISO/IEC 27701:201...". Click [here](#) to purchase the full version from the ANSI store.

This is a preview of "DS/ISO/IEC 27701:201...". Click here to purchase the full version from the ANSI store.

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

1 Scope

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to [ISO/IEC 27001](#) and [ISO/IEC 27002](#) for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

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/IEC 27000](#), *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[ISO/IEC 27001:2013](#), *Information technology — Security techniques — Information security management systems — Requirements*

[ISO/IEC 27002:2013](#), *Information technology — Security techniques — Code of practice for information security controls*

[ISO/IEC 29100](#), *Information technology — Security techniques — Privacy framework*