Avaldatud eesti keeles: detsember 2025
Jõustunud Eesti standardina: detsember 2025

INFOTURVE, KÜBERTURVE JA PRIVAATSUSKAITSE
Privaatsusteabe halduse süsteemid
Nõuded ja juhised

Information security, cybersecurity and privacy protection
Privacy information management systems
Requirements and guidance
(ISO/IEC 27701:2025)

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO/IEC 27701:2025 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis jõustumisteate meetodil vastu võetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles detsembris 2025;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2025. aasta detsembrikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 04 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud Cybernetica AS ja standardi on heaks kiitnud EVS/TK 04.

Euroopa standardimisorganisatsioon on teinud Euroopa standardi EN ISO/IEC 27701:2025 rahvuslikele liikmetele kättesaadavaks 22.10.2025.

Date of Availability of the European Standard EN ISO/IEC 27701:2025 is 22.10.2025.

See standard on Euroopa standardi EN ISO/IEC 27701:2025 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardimis- ja Akrediteerimiskeskus ning sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the European Standard EN ISO/IEC 27701:2025. It was translated by the Estonian Centre for Standardisation and Accreditation. It has the same status as the official versions.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

EUROOPA STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27701

October 2025

ICS 35.030

Supersedes EN ISO/IEC 27701:2021

English Version

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance (ISO/IEC 27701:2025)

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée — Exigences et recommandations (ISO/IEC 27701:2025)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Datenschutz-Informationsmanagementsysteme — Anforderungen und Leitlinien (ISO/IEC 27701:2025)

This European Standard was approved by CEN on 4 August 2025.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Ref. No. EN ISO/IEC 27701:2025 E

SISUKORD

EUROOPA EESSÕNA 4
EESSÕNA 5
SISSEJUHATUS 6
1 KÄSITLUSALA 7
2 NORMIVIITED 7
3 TERMINID JA MÄÄRATLUSED 7
4 ORGANISATSIOONI KONTEKST 11
4.1 Organisatsiooni ja selle konteksti mõistmine 11
4.2 Huvipoolte vajaduste ja ootuste mõistmine 11
4.3 Privaatsusteabe haldussüsteemi käsitlusala kindlaksmääramine 12
4.4 Privaatsusteabe haldussüsteem 12
5 EESTVEDU 12
5.1 Eestvedu ja kohustumus 12
5.2 Privaatsuspoliitika 13
5.3 Rollid, kohustused ja volitused 13
6 PLAANIMINE 13
6.1 Riskide ja võimaluste käsitlemisele suunatud tegevused 13
6.1.1 Üldist 13
6.1.2 Privaatsusriskikontroll 14
6.1.3 Privaatsusriskide käsitlus 14
6.2 Privaatsuseesmärgid ja nende saavutamise plaanimine 15
6.3 Muudatuste plaanimine 16
7 TUGI 16
7.1 Ressursid 16
7.2 Pädevus 16
7.3 Teadlikkus 16
7.4 Kommunikatsioon 17
7.5 Dokumenteeritud teave 17
7.5.1 Üldist 17
7.5.2 Dokumenteeritud teabe loomine ja ajakohastamine 17
7.5.3 Dokumenteeritud teabe haldus 17
8 TOIMIMINE 18
8.1 Toimimise planeerimine ja ohje 18
8.2 Privaatsusriskikontroll 18
8.3 Privaatsusriskide käsitlus 18
9 SOORITUSE HINDAMINE 18
9.1 Seire, mõõtmine, analüüs ja hindamine 18
9.2 Siseaudit 19
9.2.1 Üldist 19
9.2.2 Siseauditi kava 19
9.3 Juhtkondlik läbivaatus 19
9.3.1 Üldist 19
9.3.2 Juhtkondliku läbivaatuse lähteandmed 19
9.3.3 Juhtkondliku läbivaatuse tulemid 20

10 TÄIUSTAMINE 20
10.1 Pidev täiustamine 20
10.2 Lahknevused ja parandusmeetmed 20
11 TÄIENDAV TEAVE LISADE KOHTA 20
Lisa A (normlisa) Suunised privaatsusteabe haldussüsteemiga seotud meetmete ja nende eesmärkide kohta isikutuvastusteabe vastutavatele ja volitatud töötlejatele 21
Lisa B (normlisa) Teostusjuhised isikutuvastusteabe vastutavatele ja volitatud töötlejatele 27
Lisa C (teatmelisa) Vastavused standardiga ISO/IEC 29100 62
Lisa D (teatmelisa) Vastavused andmekaitse üldregulatsiooniga 64
Lisa E (teatmelisa) Vastavused selle dokumendi ning standardite ISO/IEC 27018 ja ISO/IEC 29151 vahel 67
Lisa F (teatmelisa) Vastavused standardiga ISO/IEC 27701:2019 69
Kirjandus 74

EUROOPA EESSÕNA

Dokumendi (EN ISO/IEC 27701:2025) on koostanud tehniline komitee ISO/IEC JTC 1 „Information technology“ koostöös tehnilise komiteega CEN-CENELEC/ JTC 13 „Cybersecurity and Data Protection“, mille sekretariaati haldab DIN.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2026. a aprilliks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2026. a aprilliks.

Tuleb pöörata tähelepanu võimalusele, et dokumendi mõni osa võib olla patendiõiguse objekt. CEN-CENELEC ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

See dokument asendab standardit EN ISO/IEC 27701:2021.

Igasugune tagasiside ja küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile / rahvuslikule komiteele. Täielik loetelu nende organisatsioonide kohta on leitav CEN-i ja CENELEC-i veebilehtedelt.

CEN-i/CENELEC-i sisereeglite järgi peavad Euroopa standardi kasutusele võtma järgmiste riikide rahvuslikud standardimisorganisatsioonid: Austria, Belgia, Bulgaaria, Eesti, Hispaania, Holland, Horvaatia, Iirimaa, Island, Itaalia, Kreeka, Küpros, Leedu, Luksemburg, Läti, Malta, Norra, Poola, Portugal, Prantsusmaa, Põhja-Makedoonia Vabariik, Rootsi, Rumeenia, Saksamaa, Serbia, Slovakkia, Sloveenia, Soome, Šveits, Taani, Tšehhi Vabariik, Türgi, Ungari ja Ühendkuningriik.

Jõustumisteade

CEN-CENELEC on dokumendi ISO/IEC 27701:2025 teksti muutmata kujul üle võtnud kui EN ISO/IEC 27701:2025.

EESSÕNA

ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) moodustavad ülemaailmse standardimise kohandatud süsteemi. Rahvuslikud organisatsioonid, kes on ISO või IEC liikmed, osalevad rahvusvaheliste standardite väljatöötamisel asjakohase organisatsiooni loodud tehniliste komiteede kaudu, mille eesmärk on tegeleda konkreetsete tehniliste valdkondadega. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale organisatsioonile huvi pakkuvates valdkondades. Selles töös osalevad ka muud ISO-ga ja IEC-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaühendused.

Selle dokumendi väljatöötamiseks kasutatud ja edasiseks haldamiseks mõeldud protseduurid on kirjeldatud ISO/IEC direktiivide 1. osas. Eriti tuleb silmas pidada eri heakskiidukriteeriumeid, mis on eri liiki ISO dokumentide puhul vajalikud. See dokument on kavandatud ISO/IEC direktiivide 2. osas esitatud toimetamisreeglite kohaselt (vt www.iso.org/directives või www.iec.ch/members_experts/refdocs).

ISO ja IEC pööravad tähelepanu võimalusele, et selle dokumendi rakendamine võib olla seotud patendi (patentide) kasutamisega. ISO ja IEC ei võta seisukohta mis tahes esitatud patendiõiguste tõendamise, kehtivuse ega rakendatavuse eest. Selle dokumendi avaldamise kuupäeva seisuga ei ole ISO ega IEC saanud teateid patendi (patentide) kohta, mida võib vaja minna selle dokumendi rakendamiseks. Dokumendi kasutajaid on siiski hoiatatud, et siin esitatu ei pruugi olla uusim teave, mis võib olla saadud patendiandmebaasist (kättesaadav veebilehelt www.iso.org/patents ja https://patents.iec.ch). ISO ja IEC ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

Mis tahes selles dokumendis kasutatud äriline käibenimi on kasutajate abistamise eesmärgil esitatud teave ja ei kujuta endast toetusavaldust.

Selgitused standardite vabatahtliku kasutuse ja vastavushindamisega seotud ISO eriomaste terminite ja väljendite kohta ning teave selle kohta, kuidas ISO järgib WTO tehniliste kaubandustõkete lepingus sätestatud põhimõtteid, on esitatud järgmisel aadressil: www.iso.org/iso/foreword.html. IEC puhul vaata www.iec.ch/understanding-standards.

Dokumendi on koostanud ühiselt tehnilise komitee ISO/IEC JTC 1 „Information technology“ alamkomitee SC 27 „Information security, cybersecurity and privacy protection“ koostöös Euroopa Standardikomitee (CEN) tehnilise komiteega CEN/CLC/JTC 13 „Cybersecurity and data protection“ kooskõlas ISO ja CENi vahelise tehnilise koostöö kokkuleppega (Viini kokkulepe).

Teine väljaanne tühistab ja asendab esimest väljaannet (ISO/IEC 27701:2019), mis on tehniliselt üle vaadatud.

Peamised muudatused on järgmised:

— dokument on reorganiseeritud iseseisvaks juhtimissüsteemi standardiks.

Igasugune tagasiside ja küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav www.iso.org/members.html ja www.iec.ch/national-committees.

SISSEJUHATUS

0.1 Üldist

Sisuliselt iga organisatsioon töötleb isikutuvastusteavet (PII). Töödeldava isikutuvastusteabe maht ja liikide arv kasvab seejuures järjepidevalt; samuti suureneb järjepidevalt selliste olukordade hulk, kus organisatsioonil on isikutuvastusteabe töötluse vallas vaja teha koostööd teiste organisatsioonidega. Privaatsuse kaitsmine isikutuvastusteabe töötluse kontekstis on mitte ainult paljudes riikides sellele pühendatud arvukate õigusnormide objekt, vaid ka ühiskonna reaalne vajadus.

Dokument sisaldab vastavustabeleid, kus siin esitatud meetmed on viidud kokku järgmiste normatiividega:

— ISO/IEC 29100-s määratletud privaatsuskarkass ja -printsiibid;

— ISO/IEC 27018;

— ISO/IEC 29151;

— ELi isikuandmete kaitse üldmäärus.

MÄRKUS Vastavustabeleid on võimalik tõlgendada viisil, mis võtab arvesse kohalikke õigusnõudeid.

Siinne dokument on mõeldud kasutamiseks isikutuvastusteabe vastutavatele töötlejatele (sh kaasvastutavatele töötlejatele) ja isikutuvastusteabe volitatud töötlejatele (sh volitatud töötlejatele, kes kasutavad alltöövõtjatest isikutuvastusteabe volitatud töötlejaid ning neile, kes töötlevad isikutuvastusteavet põhitöötleja alltöövõtjana).

Dokumendis toodud nõuete täitmine võimaldab organisatsioonil genereerida asitõendeid isikutuvastusteabe töötluse kohta organisatsioonis. Sellised asitõendid võivad lihtsustada kokkulepete sõlmimist äripartneritega situatsioonides, kus isikutuvastusteabe töötlus on mõlema poole jaoks oluline. Samuti võib neist olla abi suhetes teiste huvipooltega. Siinse dokumendi rakendamine võib luua võimaluse kirjeldatud asitõendite sõltumatuks kontrolliks.

0.2 Ühilduvus teiste haldussüsteemistandarditega

Dokument rakendab ISO arendatud haldussüsteemistandardite ühtlustamise raamistikku.

Dokument võimaldab organisatsioonil lõimida või ühtlustada oma privaatsusteabe haldussüsteemi (PIMS) teiste haldussüsteemistandarditega, eelkõige ISO/IEC 27001-s esitatud infoturbe haldussüsteemiga.

1 KÄSITLUSALA

Dokument esitab nõuded privaatsusteabe haldussüsteemi (*privacy information management system*, PIMS) loomiseks, elluviimiseks, halduseks ja järjepidevaks parendamiseks.

Samuti esitab see juhiseid, mis aitavad kohaldada dokumendi nõudeid.

Dokument on mõeldud isikutuvastusteabe (PII) vastutavatele ja volitatud töötlejatele, kellel lasub vastutus ja vastutavus isikutuvastusteabe töötluse eest.

Dokument on kohaldatav igat liiki ja mis tahes suurusega organisatsioonidele, sealhulgas avalikele ja eraettevõtetele, riigiasutustele ja mittetulundusühingutele.

2 NORMIVIITED

Allpool nimetatud dokumentidele on tekstis viidatud selliselt, et nende sisu kujutab endast kas osaliselt või tervenisti selle dokumendi nõudeid. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO/IEC 29100. Information technology — Security techniques — Privacy framework

3 TERMINID JA MÄÄRATLUSED

Dokumendi rakendamisel kasutatakse allpool esitatud termineid ja määratlusi.

ISO ja IEC hoiavad alal standardimisel kasutamiseks olevaid terminoloogiaandmebaase järgmistel aadressidel:

— ISO veebipõhine lugemisplatvorm: kättesaadav veebilehelt https://www.iso.org/obp/;

— IEC Electropedia: kättesaadav veebilehelt https://www.electropedia.org/.

3.1
organisatsioon (*organization*)
isik või inimrühm, kellel on oma ülesanded ning kellel on kohustused, õigused ja suhted enda eesmärkide (3.6) saavutamiseks

MÄRKUS 1 Organisatsiooni mõiste hõlmab muuhulgas ainuomanikku, äriühingut, korporatsiooni, firmat, ettevõtet, ametiasutust, seltsingut, heategevusühingut või asutust või nende mingit osa või kombinatsiooni, olgu see tulunduslik või mitte, avalik või eraõiguslik.

MÄRKUS 2 Juhul kui organisatsioon moodustab osa mingist suuremast olemist, osutab termin „organisatsioon“ vaid privaatsusteabe haldussüsteemi (3.23) käsitlusalas olevale osale sellest olemist.

3.2
huvipool (*interested party*)
isik või organisatsioon (3.1), kes võib mingi otsuse või tegevusega mõjutada, olla sellega mõjutatav või tunduda olevat sellega mõjutatud

3.3
tippjuht; tippjuhtkond (*top management*)
isik või inimrühm, kes suunab ja juhib organisatsiooni (3.1) kõige kõrgemal tasemel

MÄRKUS 1 Tippjuhtkonnal on võim delegeerida organisatsioonis õigusi ja anda ressursse.