EESTI STANDARD EVS-EN 17529:2022

Avaldatud eesti keeles: juuni 2022
Jõustunud Eesti standardina: juuni 2022

LÕIMELINE JA VAIKELINE ANDMEKAITSE JA PRIVAATSUS

Data protection and privacy by design and by default

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN 17529:2022 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 juunis 2022;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2022. aasta juunikuu numbris.

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

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

Standardi mõnedele sätetele on lisatud Eesti olusid arvestavaid märkusi, selgitusi ja täiendusi, mis on tähistatud Eesti maatähisega EE.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN 17529:2022 rahvuslikele liikmetele kättesaadavaks 18.05.2022.

Date of Availability of the European Standard EN 17529:2022 is 18.05.2022.

See standard on Euroopa standardi EN 17529:2022 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 17529:2022. 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 17529

May 2022

ICS 35.030

English Version

Data protection and privacy by design and by default

Protection des données et de la vie privée dès la conception et par défaut

Datenschutz by Design und als Grundeinstellung

This European Standard was approved by CEN on 5 December 2021.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

Ref. No. EN 17529:2022 E

SISUKORD

EUROOPA EESSÕNA

Dokumendi (EN 17529:2022) on koostanud tehnilise komitee CEN/CENELEC JTC 13 „Cybersecurity and Data Protection“ töörühm WG 5 „Data Protection, Privacy and Identity Management“, mille sekretariaati haldab DIN.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2022. a novembriks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2022. a novembriks.

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

Dokument on koostatud CEN/CLC JTC 13 tööprogrammi osana, mitte ainult esimese ametliku dokumendina, mis on koostatud mandaadi M/530 alusel, mille on CEN-ile ja CENELEC-ile andnud Euroopa Komisjon, vaid ka piisavalt üldisena, et olla rakendatav lisaks julgeolekutööstusele, mis on mandaadi fookuses, eri valdkondades.

Teave EL-i direktiivi(de) kohta on esitatud teatmelisas ZA, mis on selle dokumendi lahutamatu osa.

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

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.

SISSEJUHATUS

0.1 Üldist

Dokument varustab komponentide ja alamsüsteemide arendajad varakult formaliseeritud protsessiga privaatsuseesmärkide ja -nõuete identifitseerimiseks ning kaasnevaks hindamiseks vajalike juhistega. Veel annab dokument tuge arusaamisel kaskaaditud vastutusest ning tootjate ja teenustajate kohustustest (mis põhineb GDPR-il ja kohaldamisnõue selle artiklil 25, samuti valitsusrakendustele kohaldatavatel reeglitel).

Isikuandmete kaitse üldmäärus oma artiklis 25 kohustab vastutavaid töötlejaid ja kaudselt tootjaid evitama lõimelise ning vaikelise andmekaitse.

Dokumendi siht on esitada nõuded tootjatele ja/või teenustajatele lõimelise ja vaikelise andmekaitse ja privaatsuse (LVAKP) evitamiseks oma toodete ja teenuste varases arendusjärgus, s.o enne iga konkreetse rakenduse integreerimist või sõltumata selle integratsioonist, eesmärgiga tagada eeldatataval turul võimalikult kõrge privaatsusvalmidus.

EN ISO 9001 kvaliteedihaldussüsteem esitab protsessiraamistiku, mille kaudu tooted ja teenused saavad kaasata lõimelise andmekaitse ja privaatsuse. Lisa C näitab, kuidas saab standardit EN ISO 9001 vajaduse korral tõlgendada ja laiendada kasutamiseks selles valdkonnas. Juhtimiseesmärgid ja nõuded on tuletatud isikuandmete kaitse üldmäärusest, mida komponendi valmistaja ja tarkvara alamsüsteemide või alamteenuste tootja peaks uurima. Need jaotised on kohaldatavad ka B2B turule, kuivõrd selliseid alamkomponente suurematesse süsteemidesse koondavad tootjad peavad oma süsteemide kavandamise osana aru saama iga komponendi võimetest ja piirangutest. Lõpuks kirjeldatakse omadeklaratsiooni mehhanismi, mida saavad komponendi valmistajad ja teenustajad kasutada süsteemiintegraatorite ees ühe osana selle komponendi või teenuse võimete, kaitsete ja piirangute atesteerimissüsteemist.

Teatud töötluseesmärkideks ning isikuandmete teatud kategooriate jaoks tuleb EN ISO/IEC 29134 kohaselt läbi viia andmekaitsealane mõjuhindamine ja lisaks selles dokumendis esitatud nõuetele ühtlasi täita mõjuhinnangust tulenev käsitlusplaan.

Dokument on mõeldud kasutamiseks tootjatele, tarnijatele, riist- ja tarkvara arendajatele, kes varustavad toodete ja teenustega süsteemiintegraatoreid, kes omakorda plaanivad pakkuda tooteid ja teenuseid vastutavatele ja volitatud töötajatele. Dokument võimaldab süsteemiintegraatoritel valida ja korrektselt kasutada alamsüsteemide ja komponendi tarnijate ning tootjate pakutut juhtudel, kui arendatavale süsteemile esitatakse andmekaitsenõudeid.

0.2 Ühtesobivus haldussüsteemistandarditega

Dokument realiseerib CEN/CENELEC-i ja ISO arendatud raamistiku oma haldussüsteemistandarditega sobitamiseks. Dokument ise haldussüsteemistandardit ei esita.

Dokument toetab organisatsiooni selle andmekaitsealaste arenduskaalutluste integreerimisel või sobitamisel haldussüsteemistandardite nõuetega.

1 KÄSITLUSALA

Dokument määratleb lõimelise ja vaikelise andmekaitse ja privaatsuse (LVAKP[1]) nõuded tootjatele ja teenustajatele evitamiseks oma toodete ja teenuste varases arendusjärgus, s.o enne iga konkreetse rakenduse integreerimist või sõltumata selle integratsioonist, eesmärgiga tagada [toodete ja teenuste] võimalikult kõrge privaatsusvalmidus. Dokument on kohaldatav kõigis ärisektorites, sh turbetööstuses.

2 NORMIVIITED

Selles dokumendis ei ole normiviiteid.

3 TERMINID JA MÄÄRATLUSED

3.1 Terminid ja määratlused

Standardi rakendamisel kasutatakse allpool esitatud termineid ja määratlusi.

ISO ja IEC hoiavad alal standardimisel kasutamiseks olevaid terminoloogilisi andmebaase järgmistel aadressidel:

— IEC Electropedia: kättesaadav veebilehelt http://www.electropedia.org/;

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

3.1.1
lõimeline andmekaitse (*data protection by design*)
andmekaitsepõhimõtete teostamiseks kavandatud tehnilised ja korralduslikud meetmed

MÄRKUS Meetmed tuleb evitada tõhusal viisil ning lõimida töötlusse.

3.1.2
vaikeline andmekaitse (*data protection by default*)
tehnilised ja korralduslikud meetmed tagamaks, et töödeldaks üksnes iga konkreetse töötlusotstarbe jaoks vajalikke isikuandmeid[2]

MÄRKUS Sellised meetmed peaksid vähimalt määratlema kogutavate isikuandmete hulga, nende töötlemise ulatuse, säilitamise kestuse ning juurdepääsetavuse.

3.1.3
andmekaitsealane mõjuhindamine (ka mõjuhinnang) (*data protection impact assessment (DPIA)*)
privaatsuse potentsiaalse mõju tuvastamise, analüüsimise, hindamise, aga ka konsulteerimise, suhtlemise ning planeerimise üldine protsess seoses isikuandmete töötlemisega ning paigutatuna organisatsiooni laiemasse riskihaldusraamistikku

MÄRKUS Vaba tõlge ISO/IEC 29134:2017, 3.7.

[1] EE MÄRKUS LVAKP – lõimeline ja vaikeline andmekaitse ja privaatsus (ingl DPPbDD, *Data Protection and Privacy by Design and by Default*).

[2] EE MÄRKUS Ingliskeelne määratlus ei anna paraku edasi kõige põhilisemat – et GDPR-i kohased meetmed peavad olema igasse lahendusse juba sisse ehitatud. Tõenäoliselt on ingliskeelne termin sedavõrd iseseletav, et ei peetud vajalikuks seda üle seletada.