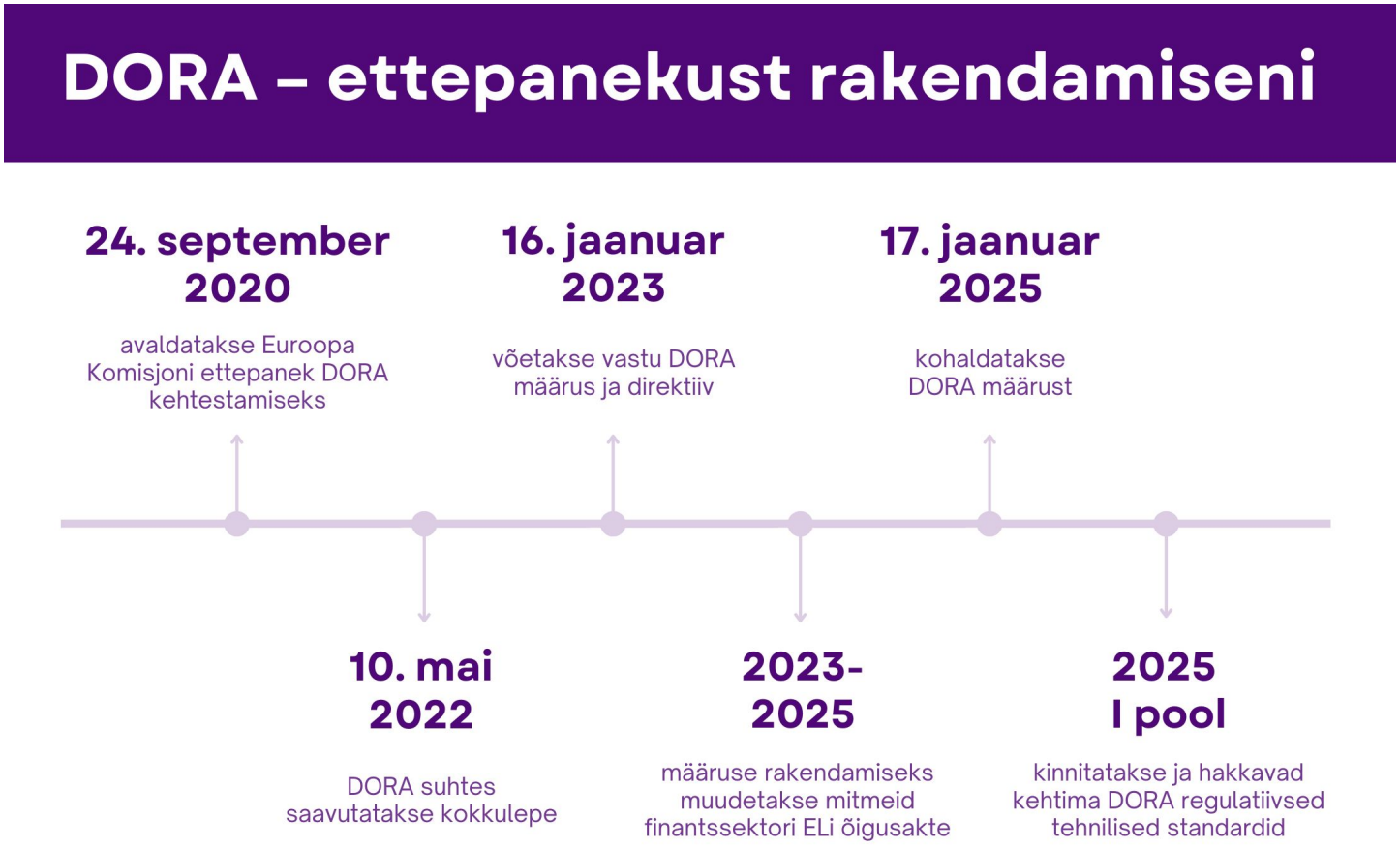
DORA määrusest ja nõuetest Eesti finantssektoris tegutsevatele ettevõtetele

Alates 2025. aasta 17. jaanuarist kohaldatakse Euroopa Liidu määrust, mis käsitleb finantssektori digitaalset tegevuskerksust (DORA) ja mida kohaldatakse suure osa finantssektori suhtes. Muudatused puudutavad nii pankasid, makseasutusi, e-raha asutusi, investeerimisühinguid, krüptovarateenuste pakkujaid ja kauplemiskohti, kindlustusandjaid ja –vahendajaid, fondivalitsejaid kui ka ühisrahastus-teenuse osutajaid. Krüptovarateenuste pakkujate puhul jäävad DORA kohaldamisalasse need, kes on saanud vastava tegevusloa.

DORA määruse eesmärk on parandada finantssektori digitaalset tegevuskerksust ja leevendada info- ja kommunikatsioonitehnoloogiaga (IKT) seotud riske. Määruses on kirjas nõuded, mis käsitlevad IKT-riskide juhtimist, IKT-intsidentide liigitamist ja nendest järelevalve teavitamist, digitaalse tegevuskerksuse testimist, kolmandast isikust tuleneva IKT-riski juhtimist, info jagamist finantsasutuste vahel jne. Kui seni on erinevates Euroopa Liidu liikmesriikides IKT riske reguleeritud erinevalt, siis nüüd põhinõuded ühtlustuvad.



INTSIDENTIDEST TEAVITAMINE

DORA III peatükk sätestab nõuded, mis puudutavad IKT- intsidentide haldamist, liigitamist ja nendest järelevalveasutusele teavitamist. DORA kohaldumisalasse kuuluvad finantsasutused peavad teavitama Finantsinspektsiooni tõsistest IKT-intsidentidest ja olulistest küberohtudest. Samad teatamise nõuded kehtivad ka maksetega seotud intsidentide ning tõsiste intsidentide kohta, kui need mõjutavad krediidi- ja makseasutusi ning e-raha asutusi.

Tõsiste IKT-intsidentide ja oluliste küberohtude teated, samuti tegevust või turvalisust mõjutavad maksetega seotud intsidentide ja tõsiste intsidentide teated tuleb alates 17.01.2025 saata elektrooniliselt e-posti aadressile intsident@fi.ee. Kõik eelnevalt nimetatud teated palume krüpteerida DigiDoc'iga ja saata need Finantsinspektsiooni ID-kaardile „Finantsinspektsioon: Dokumendi kinnitus".

Kui on tehniliselt võimatu esitada esialgset teadet Finantsinspektsiooni poolt nõutud vormil, tuleb intsidendist teavitada Finantsinspektsiooni mõnel muul viisil.

Hetkel on intsidentidest ja küberohust teavitamise vormid saadaval inglise keeles. Aruande vorme on lubatud täita nii eesti kui ka inglise keeles.

Dora incident reporting template (xlsx, 0.13 MB)

Dora significant cyber threats template (xlsx, 65.68 kB)

Aruande vormid on uuendatud 24.01.2025. Juhime tähelepanu, et vormi protsentuaalse väärtusega lahtris toimub automaatne teisendus ja vorm eeldab komakohas punkti kasutamist. Seega võib väärtuse lisamisel esineda probleeme, kui Excel on seadistatud kasutama komakohas koma. Sellisel juhul muuta aruande täitmiseks Exceli seadeid järgmiselt: File ? Options ? Advanced aknas 'Editing options' valiku alt eemaldada linnuke 'Use system separators' kastist ja 'Decimal separator' kasti lisada koma (,) asemel punkt (.).

TEABEREGISTRITE ESITAMINE

DORA V peatükk kohustab finantsasutusi esitama järelevalveasutusele iga-aastaselt IKT teenuste lepingute kohta teaberegistrid. Finantsasutused esitavad teaberegistrid grupiüleselt kõrgeimal tasemel. Esimene teaberegister tuleb täita seisuga 31.03.2025 ja esitada vastavalt Finantsinspektsiooni juhistele. Edaspidi kogutakse teaberegistreid jaanuari lõpu seisuga (alates 31.01.2026).

Kõik IKT teenuste lepingute teaberegistri täitmisega seotud vajalikud failid on kättesaadavad Euroopa Pangandusjärelevalve kodulehel:
https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application

Lisaks leiab nimetatud lingilt materjale seoses 2024. aastal Euroopa järelevalveasutuste läbiviidud teaberegistri koostamise harjutusega – sh näidiseid teaberegistri täitmiseks, töötubade salvestused ja küsimused-vastused.

18.12.2024 toimunud töötoa salvestust soovitame vaadata kõigil DORA kohaldamisalasse jäävatel

finantssektori ettevõtjatel, isegi kui nad eelnevast harjutusest osa ei võtnud. Viimase töötoa salvestuses tutvustatakse lisaks harjutuse kokkuvõttele ka teaberegistri failidesse sisse viidud muudatusi ja olulisi tähelepanekuid teaberegistri täitmise kohta.

Juhime tähelepanu, et Euroopa Komisjoni kinnitatud failide vormid erinevad harjutuse jaoks mõeldud failide vormidest ning viimaseid ei tohi kasutada teaberegistrite täitmiseks ja esitamiseks Finantsinspektsioonile.

REGULATIIVSED STANDARDID JA SUUNISED

Euroopa Komisjoni poolt kinnitatud ja Euroopa Teatajas avaldatud regulatiivsed standardid:

- *RTS on ICT risk management framework and on simplified ICT risk management framework*
  Regulatiivne tehniline standard, millega määratakse kindlaks IKT-riski juhtimise vahendid, meetodid, protsessid ja põhimõtted ning lihtsustatud IKT-riski juhtimise raamistik
  https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32024R1774
- *RTS on criteria for the classification of ICT-related incidents*
  Regulatiivne tehniline standard, millega määratakse kindlaks IKT intsidentide ja küberohtude liigitamise kriteeriumid, kehtestatakse olulisuse läved ja täpsustatakse tõsiste intsidentide kohta esitatavate raportite üksikasju
  https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=OJ:L_202401772
- *ITS to establish the templates for the register of information*
  Rakenduslikud tehnilised standardid seoses teaberegistri standardvormidega
  https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32024R2956&qid=1734516630203
- *RTS on the policy on ICT services supporting critical or important functions provided by ICT third-party service providers*
  Regulatiivne tehniline standard täpsustamaks põhimõtete üksikasjalikku sisu seoses lepingutega, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist
  https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32024R1773
- *ITS on the content, format, templates and timelines for reporting major ICT-related incidents and significant cyber threats*
  Link lisatakse avaldamisel

Euroopa Komisjoni poolt seisuga 16.12.2024 veel kinnitamata regulatiivsed standardid:

- RTS on the content, format, templates and timelines for reporting major ICT-related incidents and significant cyber threats
- *RTS on threat-led penetration testing*
- *RTS on the harmonization of conditions enabling the conduct of the oversight activities*
- *RTS specifying the criteria for determining the composition of the joint examination team*

Finantsinspektsiooni veebilehel avaldatud suunis:

- **Ühissuunised järelevalvealase koostöö ja teabevahetuse kohta Euroopa**

järelevalveasutuste ja pädevate asutuste vahel
https://www.fi.ee/et/juhendid/pangandus-ja-krediit/euroopa-jarelevalveasutuste-uhissuuniste-jarelevalvealase-koostoo-ja-teabevahetuse-kohta-euroopa

Ülevõtmise protsessis olevad suunised:

- *GL-s on the estimation of aggregated costs/losses caused by major ICT-related incidents* (Ühissuunised tõsiste IKT-intsidentide tekitatud aasta kogukulu ja -kahju hindamise kohta)

Kõik veel avaldamata regulatiivsed materjalid saab alla laadida Euroopa Pangandusjärelevalve kodulehelt:

https://www.eba.europa.eu/publications-and-media/press-releases/esas-published-second-batch-policy-products-under-dora

Viimati muudetud 24.01.2025