STERA ANDMETURBE PÕHIMÕTTED

Need põhimõtted kirjeldavad Stera kontserni (edaspidi: Stera)
andmeturbe põhimõtete eesmärki ning vastutusalasid ja korraldust.

Neis põhimõtetes tähendab andmeturve andmete konfidentsiaalsuse, terviklikkuse ja kasutatavuse tagamist, olenemata sellest, millisel kujul andmed on. Need põhimõtted määratlevad andmeturbe põhinõuded ja loovad aluse põhimõtteid järgiva tegevuse kavandamiseks ja elluviimiseks. Põhimõtete elluviimise toetamiseks koostatakse ka täpsemad juhised andmeturbe erinevate valdkondade jaoks.

Andmeturvet rakendatakse ja arendatakse riskikeskselt, kasutades asjakohaseid ja kulutõhusaid lahendusi. Andmeturbe põhimõtete asjakohasust hindab kord aastas Stera kontserni andmehalduse juhtimistiim.

Andmeturbe põhimõtted koos Stera väärtuste, riskijuhtimis-, turbe- ja andmekaitsepõhimõtetega on Stera hea valitsemistava oluline osa.

Andmeturbe põhimõtete eesmärk

Andmeturbe esmane eesmärk on Stera kontserni vastutusel olevate tegevuste järjepidevuse tagamine igasugustes tingimustes. Eesmärgipärane ja efektiivne andmeturve teeb võimalikuks Stera tegevusega seotud IKT-lahenduste kasutatavuse, protsessides ja teenustes kasutatavate andmete terviklikkuse ja konfidentsiaalsuse igasugustel tingimustel kõigis tegevusriikides. Need põhimõtted loovad aluse Stera kontserni infosüsteemide ja andmetöötluse turvalisuse tagamiseks.

Steras on klienditeabest ning muudest digitaalsetest funktsioonidest tekkivate ja töödeldavate andmete turvamine oluline osa vastutustundlikust tegevusest, mida Steralt eeldavad nii kliendid kui ka partnerid. Üha laienev digitaliseerumine tähendab, et ka andmeturvet reguleeritakse üha enam ka seadustega. Kõik Stera kontserni töötajad kõigis tegevusriikides peavad järgima andmeturbe põhimõtteid, neid täiendavaid printsiipe ja juhiseid ning kehtivaid õigusakte.

Andmeturbe rakendamine

Riskianalüüs

Andmeturbe riske hinnatakse ja analüüsitakse regulaarselt, lähtudes nende mõjust äritegevusele. Riskianalüüs tuleb koostada ka uute süsteemide määratlemise etapis ja seoses oluliste muudatustega, mis mõjutavad tegevuse kriitilisust.

Andmehalduse klassifikatsioon

Steral on andmehalduse klassifikatsioon, mis määratleb andmete klassi ja kriitilisuse ettevõtte jaoks ning mis arvestab kasutajaõigustega.

Isikuandmete töötlemine

Andmekaitsepõhimõtete ja -juhistega määratletakse, kuidas Steras isikuandmeid töödeldakse.

Andmeturbenõuded

Stera andmeturbenõuetega määratletakse lepingupartneritelt nõutava andmeturbe miinimumtase. Vajaduse korral saab nõutavat andmeturbe taset kontrollida audititega.

Andmeturbekoolitus

Steral on töötajate andmeturbealase teadlikkuse tõstmiseks kasutusele võetud erinevad meetmed, mida regulaarselt rakendatakse. Nende hulka kuuluvad näiteks veebikoolitus, petusõnumite simulatsioonid ja uudised siseveebis. Lisaks korraldatakse valitud sihtrühmadele suunatud andmeturbekoolitusi. Koolituste plaanimine toimub osaliselt koostöös personalitiimiga. Edasisi koolitusi plaanides võetakse arvesse töötajate kompetentsimaatriksite täitmist vajalikus osas ja andmeturvet.

Järelevalve ja seire

Andmeturbetaseme tõstmine ja hoidmine eeldab infosüsteemide toimimise süsteemset ja pidevat, automaatset jälgimist. Järelevalvet tegevad isikud on seaduse järgi kohustatud hoidma oma töös töödeldava teabe konfidentsiaalsena.

Andmeturbe olukorrast teatatakse tavapärase sisejärelevalve ning sise- ja väliskontrollide käigus. Tehnilist andmeturvet hinnatakse pidevalt ning olulisematele keskkondadele tehakse eraldi andmeturbe kontrolle.

Andmeturbejuhtumite käsitlemine

Steral on olemas protseduurid ja teenused andmeturbejuhtumite tuvastamiseks. Võimalike andmeturberikkumiste käsitlemine toimub andmehalduse osakonnas ja neist teatatakse kontserni juhtkonnale.

Andmeturberikkumised

Andmeturbepõhimõtete ja -juhiste vastane tegevus loetakse andmeturberikkumiseks.

Vastutusalad ja korraldus

Andmeturbe põhimõtted kinnitab Stera kontserni juhtkond.

Andmeturbe põhimõtted kehtivad Stera ettevõtete tegevusele kõigis Stera tegevusriikides. Stera töötajad peavad põhimõtteid järgima. Stera ettevõtted ja üksused tagavad oma tegevuses põhimõtete järgimise ja selleks vajalikud ressursid.

Tegevjuht vastutab selle eest, et Steral on riskijuhtimissüsteemi osana toimiv andmeturve. Andmeturbe rakendamisel abistab tegevjuhti kontserni andmehalduse osakond. Andmehalduse osakond töötleb ja jälgib kontserni andmeturbe riske ja riskijuhtimismeetmete rakendumist ning annab nende kohta aru kontserni juhtkonnale.

Andmeturbe rakendamise eest vastutavad kontserni juhtkonna liikmed. Andmehalduse osakond koordineerib ja arendab andmeturbe protsesse, vastutab koos teenusepakkujatega praktilise rakendamise eest, vastutab aruandluse eest ning koos äritegevuse ja ühistöö osakonnaga tuvastab andmeturberiske ja määrab nende haldamise meetmed. Iga Stera töötaja peab tuvastama andmeturbega seotud riskid, mis mõjutavad tema tööd või kontserni üldiselt, ning neile reageerima. Koolituste katvust ja kohandamist jälgitakse koostöös Stera enda personalitiimiga.

Andmeturbe juhtimine

Andmeturbe juhtimismehhanismina on kasutusel jätkuvusmudel (BCP), millest andmeturve moodustab omaette osa. Vastavalt oma töökorraldusele jälgib ja hindab Stera kontsernijuhtkond muuhulgas Stera sisekontrolli, siseauditi ja jätkuvusmudeli efektiivsust. Kontserni juhtkond koos IT-tiimiga tegeleb kontserni olulisemate andmeturberiskidega.

Jõustumine

Kinnitanud Stera kontserni juhtkond, Turu 12.12.2022.