ANDMEKAITSE INSPEKTSIOON

Lp Gerda Šein
juhtiv dokumendihaldur
Rail Baltic Estonia OÜ

gerda.sein@rbe.ee

Teie 14.11.2025

Meie 01.12.2025 nr 2.2-9/25/3736-2

Vastus selgitustaotlusele

Andmekaitse Inspektsioon (AKI) sai Teie pöördumise, milles soovite AKI selgitusi selle kohta, kas ja millises osas kohaldub Rail Baltic Eesti OÜ-le (RBE) avaliku teabe seadus (AvTS) ning mida ettevõte peab jälgima, et dokumentatsioon ja andmed oleksid seaduspäraselt hoitud ja kaitstud. Kuna küsimused on üldised, siis saame anda ka väga laiapõhjalised selgitused.

Kas ja millises osas kohaldub ettevõttele AvTS?
Märgime, et RBE-le eraõigusliku juriidilise isikuna kohaldub AvTS üksnes neis olukordades, mil ettevõte on AvTS-i mõistes teabevaldaja. Selgitame, et RBE on teabevaldaja ainult kindlatel juhtudel. Esiteks, AvTS § 5 lõikest 2 tulenevalt laienevad eraõiguslikule juriidilisele isikule teabevaldaja kohustused, kui isik täidab seaduse, haldusakti või lepingu alusel avalikke ülesandeid – ehk siis teabe osas, mis puudutab avalike ülesannete täitmist. Teiseks, teabevaldajaga võrdsustatakse äriühing teabe osas, mis puudutab riigi või kohaliku omavalitsuse eelarvest avalike ülesannete täitmiseks või toetusena antud vahendite kasutamist AvTS § 5 lg 3 punkti 2 alusel.

Seega on RBE teabevaldajaks ainult teabe osas, mis puudutab avalike ülesannete täitmist või riigi või kohaliku omavalitsuse eelarvest saadud vahendite kasutamist. Muus osas ettevõttele teabevaldaja kohustused ei laiene. Kuna AKI-le arusaadavalt rahastatakse RBE tegevust raudteetrassi ja sinna juurde kuuluvate rajatiste ehitamisel riigieelarvelistest vahenditest ning Euroopa Liidu kaasrahastusest, siis see tähendab, et selle raha kasutamist puudutavas osas on ettevõte teabevaldaja ehk peab järgima teabevaldajale AvTS-ist tulenevaid kohustusi.

Juhime RBE tähelepanu sellele, et näiteks dokumendiregistri pidamise kohustus (AvTS § 11 lg 1) ettevõttele ei laiene. Küll aga tuleb vastata asutusele edastatud teabenõuetele (AvTS 3. peatükk) ning seadusest tuleneval alusel (AvTS § 35 lg 1 või eriseadus) seada teabele juurdepääsupiirangud. Põhjalikemate suunistega selle kohta, mis osas eraõiguslik juriidiline isik on teabevalda ja millised kohustused see ettevõttele kaasa toob, saate tutvuda AKI koostatud eraõiguslike avaliku teabe valdajate juhendist.

Mida peab jälgima, et ettevõtte dokumentatsioon ja andmed oleksid seaduspäraselt hoitud ja kaitstud?
Ettevõte peaks looma selged sisemised reeglid ja protsessid, mis kirjeldavad andmete ja dokumentide kogu elukaart: loomist, kasutamist, säilitamist ja hävitamist. Nende reeglite eesmärk on tagada, et andmeid töödeldakse turvaliselt, vastutustundlikult ja kehtivaid seadusi järgides. Kirja tuleks panna selged juhised, kuidas dokumente ja andmeid luuakse ning millise

konfidentsiaalsusastmega need on. Klassifitseerimine aitab otsustada, kes tohib dokumente näha ja kuidas neid kaitsta. Näiteks ettevõttesiseselt avalik, mida võivad näha kõik töötajad. Või piiratud juurdepääsuga – dokument, millele ligipääs on ainult kindlatel töötajatel, lähtudes nende tööülesannetest. Iga klassifikatsiooniga peaks kaasnema juhised kaitsemeetmetest (näiteks krüpteerimine või rangemad ligipääsuõigused).

Samuti tuleb määrata, kui kaua dokumente säilitatakse. Säilitamistähtajad tulenevad näiteks seadustest, lepingulistest kohustustest, ettevõtte enda vajadustest. Andmete ja dokumentide elukaare viimane etapp on korrektne hävitamine. Ettevõte peab looma selged korralduslikud ja tehnilised meetmed, et digitaalsete dokumentide kustutamine on pöördumatu. Tundliku sisuga teabe kustutamisel võiks maha jääda kontrolljälg (eraldi vormistatud akt või logi). Paberdokumentide hävitamiseks kasutada näiteks ristpõikpurustajat. Suuremate koguste või konfidentsiaalsete dokumentide puhul kasutada väliseid käitlejaid, kellega peab olema leping ja kes tagavad turvalise hävitusprotsessi.

Andmetele või dokumentidele ligipääsuõigused peavad põhinema tööülesannetel - kes tohib dokumenti avada, millisel tasemel (lugemine, muutmine, kustutamine), kes vastutab õiguste andmise ja eemaldamise eest (nt uute töötajate liitumisel või lahkumisel). Kõik ligipääsud peaksid olema logitavad. Elektrooniliste ligipääsude puhul ei piisa pelgalt paroolist. Turvaline juurdepääs peaks hõlmama mitmetasandilist autentimist (MFA) – näiteks parool + mobiilirakenduses kuvatav ajutine kood või eID-vahend (ID-kaart, Mobiil-ID, Smart-ID),

Ettevõte peab teadma ja dokumenteerima, milliseid IT-lahendusi andmete töötlemiseks kasutatakse. Olgu selleks failiserverid, pilvelahendused, e-posti teenused, ärirakendused (ERP, CRM), varunduslahendused. Iga süsteemi kohta tuleks kirjeldada, kes vastutab selle haldamise eest, kuidas tagatakse turvalisus (krüpteerimine, logid, ligipääsuõigused). Kui ettevõte annab andmetöötluse osaliselt või täielikult üle välisele partnerile, tuleb kontrollida, kus toimub andmetöötlus ehk teenusepakkuja serverite või andmekeskuste asukoht (EL või kolmandates riikides). Isikuandmete puhul sõlmida andmetöötlusleping, mis vastab isikuandmete kaitse üldmääruse (IKÜM) artikkel 28 nõuetele. Enne lepingu sõlmimist hinnata teenusepakkuja turvameetmeid ja nende sobivust.

Iga ettevõte puutub reeglina kokku isikuandmetega – olgu selleks siis oma töötajate või klientide andmed. Sel juhul tuleb igas andmetöötlusprotsessis läbivalt järgida IKÜM nõudeid. IKÜM artikkel 5 lõige 1 punkt f kohaselt peab ettevõte tagama, et isikuandmeid töödeldakse viisil, mis kaitseb volitamata juurdepääsu ja ebaseadusliku töötlemise eest, väldib juhuslikku kaotamist, hävitamist või kahjustamist, kasutab sobivaid tehnilisi ja organisatsioonilisi meetmeid (nt MFA, krüpteerimine, õiguste haldus, turvapoliitikad). Artikkel 32 täpsustab, et tagada tuleb infosüsteemide ja teenuste konfidentsiaalsus, terviklus, kättesaadavust ja vastupidavust. Samuti võimekust kiiresti taastada andmed füüsilise või tehnilise rikke korral (nt varukoopiad). Teha tuleb turvameetmete korrapärast testimist ja hindamist.

IKÜM artikkel 25 selgitab, et andmekaitse peab olema sisse ehitatud igasse töötlemisprotsessi. Arvestades, et isikuandmeid töödeldakse ainult vajalikus mahus ning vastavalt konkreetsele eesmärgile.

Loodetavasti saime selgitustega abiks olla.

Lugupidamisega

Karin Uuselu
jurist
peadirektori volitusel