ANDMEKAITSE INSPEKTSIOON

Lugupeetud pakiveoteenuse osutajate seires osalejad

Meie 18.12.2024 nr 2.1.-4/23/1015-3224-1

Pakiveoteenuse osutajate seire kokkuvõte ja soovitused

Andmekaitse Inspektsioon (AKI) algatas isikuandmete kaitse üldmääruse (IKÜM) artikkel 58 ja isikuandmete kaitse seaduse § 56 alusel omaalgatusliku seire, mille eesmärk oli kaardistada pakiveoteenuse osutajate ja nendele SMS või e-posti vahendusteenuse osutajate poolt isikuandmete töötlemisega kaasnevad võimalikud kitsaskohad klientide teavitamisel.

Seire küsimustiku saatsime oktoobris 2023 viiele pakiveoteenuse osutajale – AS Eesti Post (Omniva), Itella Estonia OÜ, DPD Eesti AS, DHL Express Estonia AS ja Venipak Eesti OÜ-le. Vastasid kõik küsimustiku saajad.

Küsimustikus palusime järgnevate teavet: kas ja milliseid SMS/e-posti vahendusteenuse osutajaid pakiveoteenuse ettevõtted kasutavad ning millistes rollides ettevõte ja SMS/e-posti vahendusteenuse osutaja endid määratlevad (nt vastutav töötleja, kaasvastutav töötleja, volitatud töötleja); kas poolte vahel sõlmitud andmetöötlusleping vastab IKÜM artiklist 28 tulenevatele nõuetele; millises riigis vahendusteenuse osutaja isikuandmeid töötleb; kas vahendusteenuse osutaja kasutab omakorda alltöötlejaid; kas on tellitud või läbi viidud turvaaudit igapäevaste tegevuste kohta andmesüsteemide turvalisuse tagamisel; isikuandmete töötlemisprotsessi ja andmevahetuse kirjeldust kliendi teavitamisel paki saabumisest ning isikuandmete töötlemisregistri väljavõtet vastava töötlemistoimingu kohta.

Andmetöötlusleping ja andmetöötleja roll

Igasugune isikuandmete töötlemine volitatud töötleja poolt peab olema reguleeritud lepingu või Euroopa Liidu või liikmesriigi õiguse kohase siduva õigusakti alusel, dokument peab olema kirjalik, sh elektrooniline. Andmetöötluslepingus peavad olema üksikasjalikult kirjeldatud töötlemise sisu ja kestus, töötlemise laad ja eesmärk, isikuandmete liik ja andmesubjektide kategooriad ning poolte kohustused ja õigused[1]. Seega vahendusteenuse kasutamisel on vajalik sõlmida isikuandmete töötlemist reguleeriv leping.

Euroopa Andmekaitsenõukogu on selgitanud oma suunises 07/2020, et vastutava töötleja ja volitatud töötleja mõisted on funktsionaalsed: nende eesmärk on jaotada vastutus töötlejate tegeliku rolli kohaselt. See tähendab, et töötleja õiguslik staatus kas vastutava või volitatud töötlejana tuleb põhimõtteliselt määrata selle alusel, milline on tema tegelik tegevus konkreetses olukorras, mitte ametliku määramise teel (näiteks lepinguga). See tähendab, et rollide jagamine

[1] Andmetöötluslepingu elemendid on loetletud IKÜM artiklis 28.

peaks tavaliselt tulenema juhtumi faktiliste elementide või asjaolude analüüsist ja sellisena ei ole see läbiräägitav.[2]

Hea on tõdeda, et kõigil seires osalenud pakiveoteenuse osutajatel, kes kasutasid SMS ja/või e-posti vahendusteenuse pakkujaid, on sõlmitud kirjalikud andmetöötluslepingud. Valdavalt on pakiveoteenuse osutajad konkreetselt paki saabumisest teavitamisega seotud töötlemistoimingute osas end määratlenud kui vastutav töötleja ja vahendusteenuse pakkujat volitatud töötlejana. Vastustest selgus, et osad seires osalenud ettevõtted käsitlevad SMS/e-posti vahendusteenuse iseseisva vastutatava töötlejana. Tulenevalt sellest soovitame hinnata iga konkreetse töötlemistoimingu puhul vahendusteenuse pakkuja kasutamisel omavahelisi rolle. Nimelt on vastutava ja volitatud töötleja mõistetel IKÜM-i kohaldamisel oluline roll, sest nende alusel määratakse kindlaks, kes vastutab erinevate andmekaitse-eeskirjade järgimise eest.

Läbipaistvuse tagamine vahendusteenuse pakkuja kasutamisel

Igasugune isikuandmete töötlemine, sh andmete edastamine vahendusteenuse pakkujale, peab olema seaduslik, õiglane ja läbipaistev. Kui pakiveoteenuse osutaja kasutab SMS/e-posti vahendusteenust, et teavitada klienti paki saabumisest, edastab vastutav töötleja[3] isikuandmed volitatud töötlejale[4]. Sellisest andmeedastusest tuleb vastutavalt töötlejal ka andmesubjekte teavitada.[5]

Andmekaitse töörühm on oma suunistes määruse 2015/679 kohase läbipaistvuse kohta selgitanud, et kooskõlas õigluse põhimõttega peavad vastutavad töötlejad esitama vastuvõtjate kohta teavet, mis on andmesubjektide jaoks kõige olulisem. Praktikas on need tavaliselt nimega vastuvõtjad, et andmesubjektid teaksid täpselt, kellel on nende isikuandmed. Kui vastutavad töötlejad otsustavad esitada vastuvõtjate kategooriad, peaks teave olema võimalikult konkreetne, näidates vastuvõtja liigi (s.t märkides nende tegevusalad), tööstusharu, sektori või alamsektori ning vastuvõtjate asukoha.[6]

Seire raames kontrollisime andmetöötlejate veebilehel avalikult kättesaadavates andmekaitsetingimustes kajastatud teavet vastuvõtjate kohta. Andmekaitsetingimuste vaatlusest nähtus, et mõnel juhul ei olnud andmekaitsetingimustes teave vastuvõtja või vähemalt vastuvõtja kategooria kohta piisavalt konkreetselt kajastatud. Seega tuleb ettevõtetel oma andmekaitsetingimused üle vaadata ning tagada, et nendes kajastuks ka teave vastuvõtjate kohta piisavalt konkreetselt.

Isikuandmete edastamine

Isikuandmete edastamisel Euroopa Liidu ja Euroopa Majanduspiirkonna (EMP - Norra, Island, Liechtenstein) riikides, peab olema õiguslik alus, nagu seda on vaja igaks isikuandmete töötlemise toiminguks, kuid täiendavaid kaitsemeetmeid, mis tulenevad riikide vahelisest andmeedastusest, rakendama ei pea.

[2] Euroopa Andmekaitsenõukogu. Suunised 07/2020 vastutava töötleja ja volitatud töötleja mõistete kohta isikuandmete kaitse üldmääruses, ver 2.0. 07.07.2021, p 12, lk 9.
[3] IKÜM art 4 punkti 7 kohaselt on vastutav töötleja füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid.
[4] IKÜM art 4 punkti 8 kohaselt on volitatud töötleja füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.
[5] IKÜM art 13 lg 1 punkt e ja art 14 lg 1 punkt e kohaselt tuleb andmesubjekti teavitada isikuandmete vastuvõtjatest (või vastuvõtjate kategooriatest).
[6] Artikli 29 töörühm. Suunised määruse 2016/679 kohase läbipaistvuse kohta, WP 260 rev.01, lk 37.

Isikuandmete edastamisel Euroopa Liidu või Euroopa Majanduspiirkonna välisesse riiki ehk kolmandasse riiki saab edastamine toimuda kahel viisil – kaitse piisavuse otsuse alusel või sellise otsuse puudumise korral asjakohaste kaitsemeetmete alusel[7].

Kolmandatele riikidele isikuandmete edastamise kohta tuleb ka andmesubjekti läbi andmekaitsetingimuste teavitada.[8] Seejuures tuleks täpsustada IKÜM-i asjakohane artikkel, mis võimaldab andmete kolmandasse riiki edastamist, ja vastav mehhanism (nt artikli 45 kohane kaitse piisavuse otsus / artikli 47 kohased siduvad kontsernisisesed eeskirjad / artikli 46 lõike 2 kohased standardsed andmekaitseklauslid / artikli 49 kohased erandid ja kaitsemeetmed jne). Samuti tuleb esitada teave selle kohta, kus ja kuidas asjakohane dokument on kättesaadav või kust ja kuidas see saadakse, näiteks andes kasutatava mehhanismi lingi. Õigluse põhimõtte kohaselt peaks kolmandatele riikidele edastamise kohta esitatud teave olema andmesubjektidele võimalikult tähendusrikas; see tähendab üldiselt seda, et kolmandad riigid on ära nimetatud.[9]

Pakiveoteenuse osutajad kasutavad erinevaid SMS-vahendusteenuse pakkujaid, kelle tegevuskoht on nii Euroopa Liidu liikmesriigis (sh Eestis) kui ka väljaspool seda (sh kolmandas riigis). E-kirjade vahendusteenust valdavalt ei kasutata, kuna olemas on ettevõttesisene e-posti lahendus. Küll aga tuvastasime, et mõni teenusepakkuja kasutab otse või e-posti vahendusteenuse alltöövõtjana kolmanda riigi päritolu ettevõtet.

Seire raames soovisime muuhulgas teavet, kas pakiveoteenuse osutajad on enne SMS-i ja/või e-posti vahendusteenuste kasutusele võtmist selgitanud välja, kus füüsiliselt isikuandmeid töödeldakse (nt millises riigis asub teenusepakkuja server). Osa pakiveoteenuse osutajaid olid selle kindlaks teinud, osa aga mitte või tugineti vahendusteenuse osutaja kinnitusele, et töötlemine vastab andmekaitse nõuetele. Siinkohal märgime, et nii vastutaval töötlejal kui ka volitatud töötlejal on kohustus jälgida, kas isikuandmeid edastatakse Euroopa Liidust või Euroopa Majanduspiirkonnast välja ning vajaduse korral tuleb rakendada sobivad kaitsemeetmed sellisele edastusele.

Pakiveoteenuse osutajate andmekaitsetingimuste vaatlusest nähtus, et mõnel andmetöötlejal esineb puuduseid andmesubjekti teavitamisel andmete kolmandasse riiki edastamisest.

Isikuandmete töötlemise turvalisus

Digitaalses andmetöötluses on oluline töötlemise usaldusväärsus ja konfidentsiaalsus.[10] Andmetöötleja peab seejuures tagama, et andmed on täpsed ning neid ei ole juhuslikult või tahtlikult muudetud või rikutud. Konfidentsiaalsuse tagamiseks kaitstakse andmeid volitamata juurdepääsu eest, milleks rakendatakse erinevaid turvameetmeid. Turvameetmete rakendamine hõlmab nii füüsiliste meetmete kasutamist (nt lukustatud uksed) kui ka ajakohaste küberturvalisuse põhimõtete järgimist.

Kõik seires osalejad olid läbi viinud erinevaid turvaauditeid ning rakendavad oma igapäevases töös erinevaid meetmeid andmetöötlussüsteemide turvalisuse tagamiseks.

[7] Vt lähemalt IKÜM artiklid 44-50. Piisava andmekaitse tasemega riikide loetelu leiad: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[8] Teavitamise nõue tuleneb IKÜM art 13 lg 1 punktist f ja art 14 lg 1 punktist f.

[9] Artikli 29 töörühm. Suunised määruse 2016/679 kohase läbipaistvuse kohta, WP 260 rev.01, lk 37-38.

[10] Vastavalt IKÜM art 5 lg 1 punktile f tagatakse isikuandmete töötlemisel, et isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus“).

Soovitused

1. Teenusepakkuja valikul hinnake põhjalikult, kas teenusepakkuja võimaldab vastutaval töötlejal teostada piisavat kontrolli isikuandmete töötlemise nõuete järgimise osas. Hindamisel tuleb arvestada isikuandmete töötlemise olemust, ulatust, konteksti ja eesmärke ning võimalikke riske andmesubjektidele.
2. Sõlmige koostööpartneritega kirjalik andmetöötlusleping, kus muuhulgas on selgelt määratletud ka omavahelised rollid.
3. Vastutava ja volitatud töötleja vaheline leping peab sisaldama IKÜM artiklis 28 sätestatud elemente ning olema sõlmitud konkreetset andmetöötlustoiminguid silmas pidades.
4. Vastutava töötlejana olge teadlikud, kas isikuandmeid töödeldakse väljaspool Euroopa Liitu või Euroopa Majanduspiirkonda. Juhul, kui volitatud töötleja või tema alltöötleja paigutab isikuandmed kolmandasse riiki, siis andmeedastus peab vastama IKÜM-s sätestatud nõuetele.
5. Läbipaistvuse põhimõtte tagamiseks kajastage andmekaitsetingimustes muuhulgas teave andmete vastuvõtjate (või vastuvõtjate kategooria) kohta piisava konkreetsusega ning asjakohasel juhul ka teave kolmandatesse riikidesse edastamise kohta.
6. Isikuandmete edastamisel veenduge alati, et just see andmekoosseis on vajalik konkreetse eesmärgi saavutamiseks.
7. Korraldage töötajatele andmekaitsealaseid koolitusi, sh andmekaitseintsidentide tuvastamise ja teavitamise kohta.
8. Võimaldage töötajatel juurdepääs ainult sellistele andmetele, mis on vajalikud talle tööülesannete täitmiseks. Nii maandate võimalust eksimusteks andmetöötluses ja teabe jagamiseks selleks mitte õigust omavatele isikutele.
9. Andmete turvaliseks töötlemiseks[11]:
    a. Tagage kõikidest olulistest andmetest varukoopiad. Varundusel soovitame järgida 3-2-1 reeglit: olulistest andmetest kolm koopiat, mis salvestatakse kahele erinevale salvestusmeediumile ning ühte koopiat hoida süsteemiväliselt turvalises keskkonnas (st väljaspool võrku, mida töötajad infosüsteemide kasutamiseks kasutavad).
        - Varukoopiad peaksid olema krüpteeritud ja ligipääsetavad ainult volitatud isikutele, kasutades tugevaid autentimismeetodeid, näiteks mitmefaktoriline autentimine.
        - Varukoopiatest andmete taastamisvõimekust tuleb regulaarselt testida ning säilitamispoliitikat hallata, tagades, et koopiad vaadatakse üle ja uuendatakse vastavalt tehnoloogia või turvanõuete muutumisele.
    b. Kasutage infosüsteemides logimist tasemel, mis võimaldab vajadusel erinevate andmetöötlustoimingute uurimist.
        - Kasutage logiserverit, mis kogub erinevate rakenduste logid kokku ja teeb need analüüsi ja visualiseerimise kõlbulikuks.
        - Varundage logid.
        - Rakendage infosüsteemides automaatset monitoorimist, et kiiresti avastada ja reageerida igasugusele kahtlasele tegevusele.
    c. Teostage regulaarselt andmekaitse auditeid ja riskianalüüse, et tuvastada võimalikke nõrkusi ja parandada turvameetmeid.

Lugupidamisega

(allkirjastatud digitaalselt)

Virve Lans
valdkonnajuht
peadirektori volitusel

[11] Vt lisaks: Ardi Jürgens. Arvamusartikkel: Taskukohased juhised andmete turvamiseks, 17.06.2024