ANDMEKAITSE INSPEKTSIOON
Valvame, et isikuandmete kasutamisel austatakse eraelu ning et riigi tegevus oleks läbipaistev

Isikliku mobiilse seadme kasutamine töökeskkonnas

Soovituslik juhis tööandjale ja töötajatele

Kinnitatud 2014. aasta 16. juunil.

Sissejuhatus

Nutitelefonide ja tahvelarvutite (*seadmed*) kasutamine on muutunud väga populaarseks. Seadmete pakutavad võimalused ja nende suutlikkus on märgatavalt suurenenud. Tööandjad puutuvad üha rohkem kokku nii tööle asuvate kui olemasolevate töötajate sooviga kasutada isiklikus omanduses olevaid seadmeid töökeskkonnas igapäevatöö tegemiseks sh tööandja teabele juurdepääsuks, selle salvestamiseks kui ka töötlemiseks.

Kui tööandja lubab isiklike seadmetega töödelda organisatsiooni (avaliku sektori asutused, äriühingud, mittetulundusühingud, sihtasutused, avalik-õiguslik juriidilised isikud) hoitavaid isikuandmeid, tekib mitmeid küsimusi, mida tööandjal kui isikuandmete vastutaval töötlejal tuleb lahendada, et täita isikuandmete kaitse nõudeid. Vastutavale töötlejale peab alati jääma kontroll tema vastutuse alla kuuluvate isikuandmete üle, olenemata isikuandmete töötlemisel kasutatava seadme omanikust.

Andmekaitse Inspektsioon on koostanud juhise, mis aitab nii tööandjatel kui töötajatel mõista oma kohustusi ja edendada häid tavasid. Juhis annab selgitusi ja soovitusi, mida tuleb arvestada, kui tööandja lubab töötajatel kasutada isiklikke seadmeid organisatsiooni vastutusalasse kuuluvate isikuandmete töötlemisel.

Juhise koostamiseks on inspektsioon eestindanud ja kohandanud Ühendkuningriikide andmekaitseasutuse vastava dokumendi.

1. Isikuandmete kaitse

Isikliku seadme kasutamise aluseks on asjaolu, et kasutaja omab ja hooldab seadet. See tähendab, et tööandjal on tunduvalt väiksem kontroll seadme üle võrreldes sellega, mis tal oleks tavapäraselt organisatsioonile kuuluva ja organisatsiooni tagatud seadme kasutamisel. Andmete turvalisus on seega esmatähtis küsimus.

Enne isikliku seadme kasutusse lubamist peaks tööandja kui isikuandmete vastutav töötleja hindama:

- mis liiki andmeid hoitakse;
- kus võib andmeid hoida;
- kuidas andmeid edastatakse;
- andmelekke võimalust;
- isiklike ja äriliste eesmärkide segunemist;
- seadme turvasuutlikkust;
- mida teha, kui seadet omav isik lahkub töölt;
- kuidas käsitleda seadme kadumist, vargust, riket ja tugiteenuseid.

Isikuandmete kaitse seaduse (IKS) § 6 lg 6 kohaselt kohustub isikuandmete töötleja ehk tööandja järgima isikuandmete töötlemisel turvalisuse põhimõtet – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest.

Sama seaduse §-d 25 – 26 sätestavad, et isikuandmete töötleja on isikuandmete töötlemisel kohustatud:

- vältima kõrvaliste isikute ligipääsu andmetöötlusseadmetele;
- ära hoidma andmete omavolilist lugemist, kopeerimist, kustutamist jms;
- võimaldama tagantjärgi tuvastada, kes millal millele juurde pääses, salvestas, muutis või kustutas ning kellele, millal ja miks isikuandmeid edastati;
- tagama, et igaühel oleks juurdepääs üksnes talle töötlemiseks lubatud andmetele ja töötlemisviisidele;
- kujundada töökorraldus nii, et see võimaldaks täita andmekaitse nõudeid;
- tagama oma alluvuses isikuandmeid töötlevatele isikutele kohane väljaõpe.

2. Isikuandmete hoidmine

Isikliku seadmega töödeldavaid isikuandmeid võidakse hoida ühes või mitmes järgmises asukohas:

- seadmes;
- organisatsiooni võrguserveris (või muus privaatpilves[1]);
- avalikus pilves.

Pane tähele:

- **avaliku pilve puhul puudub tööandjal ja töötajal sisuline kontroll pilves hoitavate andmete üle;**
- **avalikus pilves on kontroll teenuse turvalisuse üle olulises osas pilveteenuse osutaja käes;**
- **avalikus pilves on võimalik andmeid sh isikuandmeid turvaliselt hoida ainult juhul, kui andmed on enne pilve saatmist tugevalt krüpteeritud;**
- **andmete krüpteeritud kujul avalikus pilves hoidmise lubamisel peab tööandja veenduma krüpteeringu piisavas tugevuses ning krüpteeringuks kasutatava seadme ning tarkvara sobivuses.**

Mobiilse seadme kasutamisel on andmete seadmes tugevalt krüpteerimine täna veel mõnevõrra problemaatiline, kuna vajab suuremat protsessorivõimsust ning akutoite vastupidavust.

Sellest tulenevalt tuleks seadmega avaliku pilve kasutamist andmete hoidmiseks ja jagamiseks vältida.

Olenemata isikuandmete hoidmise kohast, on tööandja kohustatud kasutusele võtma **asjakohased meetmed,** et kaitsta isikuandmeid volitamata või ebaseadusliku juurdepääsu eest, näiteks seadme kadumise või varastamise korral. See on tööandja kui vastutava töötleja kohustus.

Näiteks on levinud praktika, kus töötajad hoiavad seadmes läbisegi nii era- kui tööandja klientide kontakte.

Sellised meetmed võivad hõlmata andmetele või seadmele juurdepääsu kontrollimist salasõna või PIN-koodi kasutamisega või andmete krüpteerimist. Tuleb meeles pidada, et seadme kadumine või vargus ei ole ainus viis, mille kaudu on võimalik volitamata või ebaseaduslik juurdepääs isikuandmetele. Näiteks võib töötaja isiklikku seadet jagada pereliikmete vahel viisil, mis on sobimatu, kui seadmele on salvestatud isikuandmeid, mille vastutav töötleja on tööandja.

Kui isikuandmeid hoitakse kaugasukohas sh organisatsiooni sisevõrgus või avalikus pilves, on oluline võtta arvesse juurdepääsuõiguste turvalisust seadme kadumise või varguse korral. Näiteks kui seadet

[1] **Pilvandmetöötluse** *(cloud computing)* korral kasutaja salvestab, varundab või töötleb andmeid kaugarvutites *(serverites),* millele kasutajal on interneti vahendusel juurdepääs spetsiaalse tarkvara abil. Tarkvara kasutusliideseks on reeglina veebilehitseja.

kasutatakse pilveteenusele juurdepääsuks ja seade lubab kasutajal jääda sessioonidevahelisel ajal sisse logituks, võib volitamata juurdepääs seadmele tuua kergesti kaasa isikuandmete volitamata avaldamise.

Seadmed võivad isikuandmete hoidmiseks või töötlemiseks pakkuda lisakaitset näiteks läbi *virtualiseerimise süsteemi*.[2] Kui tööandja tugineb sellele kui turvameetmele, peaks ta hindama, kas tal ikka on kontroll sellise lisakaitse võimaluse üle, tagamaks andmete konfidentsiaalsus ja terviklikkus. Seadmed võivad pakkuda ka võimalust lubada juurdepääsu üksnes teatavatele rakendustele või andmeliikidele, lähtudes geograafilisest asukohast, ning nõuda kõrgemat autentimistaset.

Kui töötaja hoiab seadmes isikuandmeid, siis on oluline jälgida andmete ohutut ja turvalist kustutamist juhul, kui seade müüakse või antakse üle kolmandale isikule.

Soovitused:

- **kasutage seadmete turvamiseks tugevat salasõna;**
- **kasutage krüpteerimist, et hoida andmeid seadmes turvaliselt;**
- **tagage, et seadmele juurdepääs on lukustatud ning andmed kustutatakse automaatselt, kui salasõna sisestatakse mitmeid kordi valesti;**
- **tagage, et seade lukustub automaatselt, kui te ei ole seda mõnda aega kasutanud;**
- **tagage, et töötajad teaksid täpselt, milliseid andmeid võib automaatselt või kaugteel kustutada ja mis asjaoludel;**
- **eristage tööandja nimel töödeldavad isikuandmed ja seadme omaniku (töötaja) isiklikel eesmärkidel töödeldavad isikuandmed, kasutades näiteks äri- ja isiklikuks otstarbeks erinevaid rakendusi;**
- **kaitske seadet viirusetõrje tarkvaraga.**

3. Isikuandmete edastamine

Üks andmete edastamise turvalisust mõjutav risk on vahendusrünne *(man-in-the middle attack*) või muud liiki sekkumine, mis toimub ülekandmise ajal. Tähelepanuta ei tohiks jätta ka teisi edastamisega seotud riske, näiteks e-kirja saatmine valele aadressile.

Kui töötaja kasutab seadet tööülesanneteks väljaspool tööandja sisevõrku, peaks ta arvestama, et avalikud võrgud, näiteks Wi-Fi, ei ole üldjuhul piisavalt turvalised. Samas traadita kohtvõrgus viibivad teised kasutajad võivad näiteks pahatahtlikult püüda juurde pääseda töötaja seadme sisule. Suurimaks ohuks avalikes võrkudes on andmesideühenduse pealtkuulamise risk. See tähendab, et igaühele on vabalt pealtkuulatav kogu andmestik, mida seade võrgu vahendusel kolmanda osapoolega vahetab. Olgu selleks siis võrgulehtede külastamine või turvamata e-posti ühendus.

[2] **Virtualiseerimise süsteemid** kaitsevad seadet, käivitades tarkvara simuleeritud keskkonnas ehk „liivakastis“ (sandbox). Virtuaalne keskkond võib olla tekitatud seadmes endas või eemalasuvas serveris (terminal-lahendus). Tugevama kaitse tagab terminal-lahendus - iga kahjulik tegevus, mis pahavara teeb, teostatakse simuleeritud süsteemis ja see ei mõjuta tegelikke seadme faile ja kasutaja tähtsaid andmeid. Seadmes tekitatud virtuaalne keskkond aga ei taga pahavara kahjuliku tegevuse piisavat eraldatust seadme toimimisest ja seadmes olevatest andmetest.

Isikuandmete edastamiseks avalikes võrkudes peaks tööandja võimaldama töötajal kasutada krüpteeritud kanalit. Näiteks virtuaalse privaatvõrgu VPN lahendusi[3] või turvalist hüperteksti edastusprotokolli HTTPS.

Ka pilveteenuste kasutamine (e-post, sotsiaalvõrgustikud) võib ohustada isikuandmete edastamist kuna pilveteenuste puhul on kontroll turvalisuse üle olulises osas teenuseosutaja käes.

Samuti peaks tööandja reguleerima isikuandmete tööalase edastamise lubamise või keelamise sinihamba *(bluetooth*) või teiste lähivälja raadioside (*NFC, RFID*) lahenduste kasutamisel. Ka siin on ohuks raadioside pealtkuulamise võimalus või võimalus ühenduda soovimatu (vale) seadme või võrguga.

Mõned seadmed võimaldavad automaatset andmete varundamist kas seadmesse endasse või töötaja isiklikule pilvepõhisele kontole. Tööandjal kui isikuandmete vastutaval töötlejal tuleb tagada, et selle võimaluse lubamine ei tooks kaasa isikuandmete nõuetevastast töötlemist sh isikuandmete volitamata avaldamist või edastamist kolmandatele isikutele.

Andmete varundamist avalikus pilves tuleks vältida (vt lk 5 selgitusi).

Soovitused:

- **isikuandmete edastamine krüpteeritud kanali kaudu pakub maksimaalset kaitset;**
- **kasutage avaliku pilve põhist jagamist ja avalike varukoopiate loomise teenuseid, mida te ei ole täies ulatuses hinnanud, äärmise ettevaatusega, kui üldse.**

4. Kontroll ja turvalisus

Tööandjale on töötaja isikliku seadme kadumine või vargus peamine isikuandmete volitama töötlemise riskitegur. Põhjuseks tööandja kontrolli puudumine töötajale kuuluva seadme üle. Seepärast peaks tööandja varakult läbi mõtlema võimalikud sammud, tagamaks seadmes hoitavate isikuandmete konfidentsiaalsus. Samuti tuleks tööandjal arvestada, kuidas ta haldab töötajate isiklikes seadmetes hoitavaid andmeid sh isikuandmeid, kui töötaja lahkub töölt.

Enamik tänapäevaseid seadmeid pakub võimalust määrata kaugteel nende asukohta ja kustutada vajaduse korral seadmes olevad andmed. Seda saab teha kolmanda osapoole tarkvara ehk mobiiliseadme haldussüsteemi (*Mobile Device Management)* abil.

Teenuse kasutamise eeldus:

- seade on haldussüsteemis registreeritud;
- seade on sisse lülitatud;
- seade asub võrgu levialas.

[3] **Virtuaalne privaatvõrk ehk VPN** (ingl k *Virtual Private Network*) võimaldab turvalise ühenduse privaatvõrguga (nt tööandja või kooli võrguga). Turvalise VPN (*secure* VPN) tehnoloogia puhul edastatakse avalike võrkude kaudu krüpteeritud andmeid. Andmed krüpteeritakse päritoluseadmes ja krüpteering eemaldatakse sihtkoha lõppseadmes. Isegi kui kolmas osapool ühendust jälgib, puudub tal võimalus andmeid lugeda või muuta.

Mobiiliseadme haldussüsteemi teenused võimaldavad jälgida seadet reaalajas.

Tööandjal tuleb tagada, et kaugteel asukoha määramise teenuse raames kogutud andmeid kasutatakse üksnes kindlaksmääratud eesmärgil ning mitte töötajate pidevaks jälgimiseks. Tööandja on kohustatud seadme kasutajaid teavitama, kas ja kuidas toimub seadme jälgimine.

Tööandja peaks veenduma võimalustes, mis tagavad, et töötaja isikliku seadme operatsioonisüsteemi või muu tarkvara nõrgad kohad on asjakohaselt paigatud või ajakohastatud. Samuti peaks tööandja olema teadlik, et turvauuendused võivad sõltuda seadme tootjast või sideteenuse pakkujast (nt mobiilsideoperaator) ja mitte otseselt operatsioonisüsteemi tootjast. Lisaks ei pruugi tarkvarauuendused olla viivitamata kättesaadavad või ei ole mõne seadme puhul üldse kättesaadavad. Ükski selline probleem ei tohi ohustada isikuandmete töötlemist.

Tööandja peaks teadvustama ohte, kui töötaja „häkib“ teadlikult oma seadet (*root or jailbreak*), s.o protsess, mille käigus võidakse kõrvaldada teatavad operatsioonisüsteemi turvaseadete vaikeväärtused. Tööandjal muutub taolises olukorras seadme üle kontrolli omamine praktiliselt võimatuks. **Isikliku seadme kasutamisel tööülesannete täitmiseks peab seadme „häkkimine“ olema keelatud.**

Samuti võib tööandjal tekkida vajadus teha kindlaks, kes on volitatud paigaldama seadmele kolmandate isikute tarkvara (rakendusi). Mõned seadmed võimaldavad omanikel paigaldada ebausaldusväärsetest ja kontrollimata ostukohtadest pärit rakendusi. Taolistes ebausaldusväärsetes allikates võib pahavara esineda suurema tõenäosusega. Oluline on ka mitte üle hinnata nii-öelda ametliku ostukoha pakutavaid garantiisid. Sellised ostukohad võivad pakkuda rakenduse kohta üksnes pealiskaudset ülevaadet ega pruugi blokeerida kõiki pahavara esinemisi.

Tööandjal tuleb hinnata, kuidas ta vastutava töötlejana haldab ja kaitseb isikuandmeid juhul kui töötaja viib isikliku seadme remonti, tagastab garantii alusel tootjale või hoopis müüb.

Soovitused:

- **registreerige seadmed, et neil saaks kasutada kaugteel asukoha määramise ja andmete kustutamise teenust, tagamaks andmete konfidentsiaalsus kadumise või varguse korral;**
- **tagage, et tööandjana on teil kehtestatud protsess seadme või kasutaja juurdepääsu kiireks ja tõhusaks takistamiseks, kui teatatakse seadme kadumisest või vargusest;**
- **lubage kasutada üksnes selliseid seadmeid, mida olete hinnanud ja mis tagavad töödeldavate isikuandmete nõutava turvalisuse;**
- **andke töötajatele suuniseid riskide kohta, mis kaasnevad ebausaldusväärsete või kontrollimata rakenduste allalaadimisega.**

5. Seadme kasutamise reeglid

Tööandja peaks koostama isikliku seadme kasutamise reeglid. Selles dokumendis tuleks muuhulgas kirjeldada andmete sh isikuandmete edastamise protsess isikliku seadme ja tööandja infosüsteemide vahel. Protsess peaks kirjeldama ka riske, eriti kui tegemist on suures mahus tundliku teabega sh delikaatsed isikuandmed (IKS § 4 lg 2).

Tõhus isikliku seadme kasutamise poliitika võib tuua mitmesugust kasu, sealhulgas tagada töötajate suurema rahulolu tööga, üldise moraali paranemise, tööviljakuse kasvu ja suurema paindlikkuse. Võttes algusest peale arvesse privaatsust mõjutavaid riske, on tööandjal võimalus lõimida isikuandmete kaitse oma tööprotsessi ning täiendada üldisi nõudeid, näiteks määrata kindlaks isikuandmete koosseis, mida võib seadmes hoida. Või näiteks keelata eriti tundlike andmete salvestamise või lubada neid salvestada üksnes seadmetel, millel on kõrge krüpteerituse tase.

Enne reeglite koostamist peaks tööandja auditeerima töödeldavate isikuandmete liike ja nende salvestamiseks kasutatavaid seadmeid, sealhulgas seadmete kuuluvust. Oluline on teha kindlaks, milliseid isikuandmeid võib isiklikul seadmel töödelda ning milliseid tuleb hoida piiratumas keskkonnas. Samuti tuleb arvestada, kas töötaja isikliku seadme kasutamine tähendab, et lõppkokkuvõttes töötleb tööandja organisatsioonivälist teavet seadme omaniku ja teiste võimalike seadme kasutajate (nt pereliikmete) kohta.

Tööandja peaks hindama isikliku seadme kasutamise mõju teenustele, mida tööandja jagab teiste organisatsioonidega, ning kas see on olemasolevate kokkulepetega vastuolus või mitte.

Isikliku seadme kasutamine ei tohi nõrgestada olemasolevate teenuste turvalisust.

Isikliku seadme kasutamise reeglid võivad tuua kaasa parema andmete eraldatuse. Näiteks võib tööandja kehtestada piiranguid organisatsiooni sisevõrgust ligipääsetavatele teenustele ja võrgulehtedele. Nii väheneb andmelekke tõenäosus ja organisatsiooni infosüsteemide kohatu kasutamine. Alternatiivina võib organisatsioon luua traadita kohtvõrgu, mis on sisevõrgust eraldatud ja lubada töötajatel isiklike seadmetega seda kasutada.

Isikliku seadme kasutamise reeglid peaksid lisaks arvestama olukordadega, kus:

1) isikliku seadme kasutamine võib suurendada riski, et isikuandmeid töödeldakse muul eesmärgil kui see, milleks need on kogutud. Tööandjana peate tagama, et seadmete kasutajad teavad oma kohustust kasutada organisatsiooni valduses olevaid isikuandmeid üksnes tööalastel eesmärkidel;
2) kui andmete sh isikuandmete koopiaid hoitakse mitmes eri seadmes (tööarvuti, isiklik seade) on oht, et isikuandmed muutuvad aja jooksul aegunuks või ebatäpseks. Samuti on suurem risk, et andmeid hoitakse alles kauem kui vajalik, kuna koopiatest puudub ülevaade. Seadmete ühendamine organisatsiooni keskse IT-taristuga (näiteks andmeaidaga) võib aidata seda riski maandada.
3) võib esineda isikuandmete lekke risk, st andmed võivad juhuslikult kaduda või avalikuks saada töötaja ja tööandja teadmata. Näiteks võivad andmed jääda kopeerimisel ja kleepimisel lõikelauale (*clipboard*), mille sisu töötaja postitab kogemata sotsiaalvõrgustikku või edastab e-posti teel aadressraamatus olevatele kontaktidele.

Tulenevalt organisatsioonile kehtivatest muudest õigusaktidest ja/või regulatsioonidest tuleb organisatsiooni juhtkonnal ka neid isikliku seadme kasutamise reeglite koostamisel arvestada.

Soovitused:

- **rakendage isikliku seadme kasutamise reeglid ja hoidke need asjakohased;**
- **analüüsige organisatsiooni vajadust sotsiaalmeedia poliitika järele, kui isikliku seadme kasutamine toob kaasa sotsiaalmeedia ulatuslikuma kasutamise;**
- **sätestage selgelt, mis liiki isikuandmeid võib isiklikel seadmetel töödelda ja milliseid mitte;**
- **kaasake reeglite väljatöötamisse kõik asjaomased osakonnad (sh IT- ja personaliosakond) ning lõppkasutajad (töötajad).**