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

Infoturve ja isikuandmete kaitse väikeettevõttes

Sissejuhatus 3
1. Riskide mõjuhinnang 4
2. Mitmetasandiline turvapoliitika 5
2.1. Füüsilised turvameetmed 5
2.2. Viirus- ja pahavaratõrje 6
2.3. Sissetungimiskaitse 6
2.4. Juurdepääsukontroll 6
2.5. Töötajate teadlikkus ja koolitus 6
2.6. Segmenteerimine 7
2.7. Seadmete tugevdamine 7
3. Andmete turvalisus 7
4. IT-süsteemi ajakohastamine 8
5. Probleemide jälgimine 9
6. Kohustuste teadvustamine 9
7. Isikuandmete minimaalsus 10
8. IT-partneri kontroll 10

Sissejuhatus

Ettevõtte andmehalduse ja infosüsteemide turvalisuse tagamine nõuab aega, ressursse ja eriteadmisi. Olgu andmed kas laua- või sülearvutis, võrguserveris, pilves, mobiilses seadmes (nutitelefon, tahvelarvuti), võrgulehel, e-posti serveris või paberkandjal – kõiki neid andmeid on vaja kaitsta. Kui ettevõte töötleb isikuandmeid, siis vastutab ettevõte lisaks ka nende inimeste ees, kelle andmed tal on. Isikuandmete korral peab ettevõte teadma seadusest tulenevaid nõudeid. Ettevõte peab isikuandmete kaitseks kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed. Kehtestatud meetmed peavad vastama ettevõtte tegevusala vajadustele. Meetmed ei pruugi tingimata olla kulukad ega koormavad, vaid võivad olla suisa tasuta või IT-süsteemis juba kättesaadavad.

Andmete sh isikuandmete kaotamine või vargus võib kahjustada (1) ettevõtte mainet, (2) tuua kaasa kahjuhüvitusnõude ja (3) väärteo- või kriminaalkaristuse.

Senise praktika kohaselt eelistavad ettevõtjad hinna tõttu pigem valmis IT-lahendusi ja nn karbitooteid kui kallimaid erilahendusi. Valmis lahenduse puhul pole aga alati kindlust, kas see vastab ettevõtte vajadustele ning tagab isikuandmete töötlemisel seaduse nõuete täitmise.

Andmekaitse Inspektsioon (AKI) on koostanud juhise, mis annab ettevõtte juhtidele, infoturbe- ja IT-spetsialistidele abistavaid soovitusi andmekaitse sh isikuandmete kaitse ja infoturbe korraldamiseks ning tegevuste planeerimiseks. Kuigi isikuandmete kaitse ja infoturbe nõuded ei sõltu ettevõtte suurusest, näitab inspektsiooni kogemus vajadust oskusteabe järele just väikeettevõtjate seas. Juhise koostamiseks oleme eestindanud ja kohandanud Ühendkuningriikide andmekaitseasutuse vastava dokumendi.

1. Riskide mõjuhinnang

Enne ettevõtte andmetöötluse turvameetmete kindlaksmääramist veenduge, milliseid andmeid sh isikuandmeid te hoiate ja töötlete. Hinnake neid andmeid ohustavaid riske. Arvesse tuleb võtta kõiki andmete kogumise, salvestamise, kasutamise ja kõrvaldamisega kaasnevaid protsesse.

Seaduse kohaselt on isikuandmed mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on.[1]

Isikuandmed on näiteks ettevõtte klientide andmed nagu nimi, sugu, vanus, isikukood, e-posti aadress, elukohaandmed. Samuti on isikuandmed ettevõtte töötajate andmed sh näiteks töötaja arveldusarve number (kuhu kantakse töötasu) või andmed tööalase vormiriietuse suurusest.

Kui ettevõte töötleb isikute terviseandmeid on tegemist delikaatsete isikuandmetega.[2]

Isikuandmete töötleja on füüsiline või juriidiline isik, välismaa äriühingu filiaal või riigi- või kohaliku omavalitsuse asutus, kes töötleb või kelle ülesandel töödeldakse isikuandmeid.[3]

Isikuandmete töötlemine on isikuandmetega tehtav igasugune toiming sh isikuandmete kogumine, salvestamine, säilitamine, muutmine, avalikustamine, juurepääsu võimaldamine jms.[4]

Isikuandmeid töötlevad süsteemid on näiteks raamatupidamissüsteem (töötajate palgaarvestus), personaliarvestussüsteem (töögraafikud, tööajaarvestus, puhkused) või kliendihaldussüsteem.

Hinnake, kui väärtuslik, konfidentsiaalne või tundlik on teave ning millist kahju või milliseid probleeme võib nende lekkimine põhjustada.

Isikuandmete töötlejana peate hindama:

a) mis liiki andmeid ettevõte töötleb:
kui ettevõtte tegevus toob kaasa klientide delikaatsete isikuandmete töötlemise, tuleb delikaatsete isikuandmete töötlemine registreerida Andmekaitse Inspektsioonis.

b) kus ettevõtte andmeid hoitakse:
kas ettevõtte serverites, töötajate arvutites, mobiilsetes seadmetes, pilves.

c) ettevõtte tööruumide füüsilist turvalisust:
kas andmetöötluseks ja –edastamiseks kasutatavatele seadmetele on füüsiline ligipääs ainult selleks ettenähtud isikutel; kuidas on korraldatud tööruumidesse ligipääs ja isikute tuvastamine; kas tööruumides on mehitamata või mehitatud valve.

d) kuidas ettevõte andmeid edastab:
kas digitaalseid andmeid avatult, krüpteeritult; paberkandjal andmeid käsiposti, kulleriga.

e) andmelekke võimalust:
näiteks töötajate või koostööpartnerite hooletuse tõttu.

f) isiklike ja äriliste eesmärkide segunemist:
näiteks ettevõtte kliendibaasi kasutamine töötaja isiklikul otstarbel.

---

[1] Isikuandmete kaitse seadus § 4 lõige 1.
[2] Isikuandmete kaitse seadus § 4 lõige 2 punkt 3.
[3] Isikuandmete kaitse seadus § 7 lõige 1.
[4] Isikuandmete kaitse seadus §5.

g) seadme turvasuutlikkust:
kas operatsioonisüsteem on ajakohastatud, vajalikud turvameetmed rakendatud ning tagatud on erineva turvatarkvara tugi. Hinnata tuleb nii võrguseadmeid (serverid, ruuterid jms) kui lõppkasutajate seadmeid (lauaarvuti, sülearvuti, mobiilsed seadmed).

h) kuidas käsitleda seadme kadumist, vargust, riket ja tugiteenuseid:
kas ettevõttes on olemas dokumenteeritud turvapoliitika.[5]

Seadus kohustab isikuandmete töötlejat järgima isikuandmete töötlemisel turvalisuse põhimõtet – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest.[6]

Täpsemalt peab isikuandmete töötleja:

- vältima kõrvaliste isikute ligipääsu andmetöötlusseadmetele ning andmekandjatele (sh välised kõvakettad, mälupulgad, CD- ja DVD-plaadid jms);
- ära hoidma andmete omavolilist lugemist, kopeerimist, kustutamist jms;
- võimaldama tagantjärele tuvastada, kes millal millele juurde pääses, mida salvestas, muutis või kustutas ning kellele, millal, miks ja kuidas isikuandmeid edastati;
- tagama, et töötajatel oleks juurdepääs üksnes tööülesannete täitmiseks vajalikele andmetele ja töötlemisviisidele. Mittevajalikud juurdepääsuõigused võivad lisaks konfidentsiaalsusele põhjustada probleeme ka andmete käideldavuses[7] ning tervikluses[8];
- kujundama töökorralduse selliselt, et see võimaldaks täita andmekaitse nõudeid;
- tagama oma alluvuses isikuandmeid töötlevatele isikuile kohane väljaõpe ja teavitus turvameetmete perioodilistest uuendustest.

Kui on olemas selge ülevaade riskidest, saate hakata valima vajadustele vastavaid turvameetmeid.

2. Mitmetasandiline turvapoliitika

Ükski IT-toode või valmisteenus ei paku ettevõttele täielikku turvagarantiid. Turvalisuse tagab mitmetasandiline käitumisviis, mille puhul kasutatakse koos erinevaid meetodeid, vahendeid ja tehnikaid. Sellisel juhul, kui üks tasand ei toimi, suudetakse oht teiste meetoditega tõrjuda. Turvapoliitika abil peab isikuandmete töötleja tagama turvariskide järjepideva käsitlemise sh turvalisuse tagamiseks kasutatavate meetodite ja vahendite järjepideva uuendamise.

Hea turvapoliitika on hästi toimiva töökorralduse koostisosa.

2.1. Füüsilised turvameetmed

Tööruumidesse sissemurdmisel on oht, et kolmandad isikud saavad füüsilise ligipääsu isikuandmeid sisaldavatele seadmetele. Seadmed võidakse varastada, paigaldada andmesidet või –töötlust pealt

[5] Ettevõttesisene dokument, mis kehtestab töötajatele üldised turvalisust tagavad käitumisjuhised ja juhib tähelepanu riskidele. Turvapoliitika eesmärk on kaitsta nii arvutisüsteeme ja nendes leiduvaid andmeid kui ka teadvustada füüsilist turvalisust puudutavaid ohte.
[6] Isikuandmete kaitse seadus § 6 punkt 6.
[7] Andmete õigeaegne ja hõlbus kättesaadavus selleks volitatud isikutele.
[8] Andmete põhinemine algallikal ning veendumus, et need pole hiljem muutunud või neid pole volitusteta muudetud.

kuulamist võimaldavaid lisaseadmeid või saada ligipääs olemasolevatele andmetele. Isikuandmete töötleja peab tagama, et tema hallatavates infosüsteemides hoitavad ja/või töödeldavad isikuandmed on sellise ohu eest kaitstud. Servereid tuleb hoida eraldi sobivalt kaitstud ruumis. Varundamisseadmeid ei tohi jätta järelevalveta ning kasutamise välisel ajal peavad need olema lukustatud kohas. Paberdokumente tuleb hoida lukustatud kapis või seifis.

2.2. Viirus- ja pahavaratõrje

Ettevõtte arvuteid, arvutivõrku ühendatud seadmeid ja arvutivõrgu toimimist võimaldavaid seadmeid tuleb korrapäraselt kontrollida viirus- ja pahavaratõrje või muude sobilike (nt turvavigu tuvastavate) programmide abil, et tuvastada ohte ja neid sobilike meetodite abil kõrvaldada. Tagada tuleb kasutatavate programmide ajakohastamine (uuendamine). Samad põhimõtted kehtivad ka mobiilsete seadmete kasutamisel.

2.3. Sissetungimiskaitse

Ründed IT-seadmetele (arvutid, serverid, võrguseadmed, mobiilsed seadmed) tuleb tuvastada ja tõrjuda selleks sobilike vahenditega (näiteks piisava konfiguratsiooniga tulemüür) enne, kui sissetungija on suutnud ettevõtte seadmetesse ligipääsu saavutada. Kui riski hinnates selgub, et mõnda tüüpi seadet pole võimalik rünnete eest piisavalt kaitsta (näiteks vananenud operatsioonisüsteemiga arvuti, nõrkade turvalisusseadetega nutitelefon vms), ei sobi see ka isikuandmete töötlemiseks ega ühendumiseks ettevõtte andmesidevõrguga.

2.4. Juurdepääsukontroll

Ettevõtte infosüsteemile võivad ligi pääseda vaid need isikud, kes on selleks volitatud ning koolitatud isikuandmeid töötlema. Ettevõttel peab olema ülevaade, kes, millal ning milliseid infosüsteeme või seadmeid kasutab. Iga kasutaja peab olema tuvastatav (näiteks unikaalne kasutajanimi ja parool, ID-kaardi ja/või Mobiil-ID lahendused). Vastavad nõuded tulenevad seadusest.[9]

Väga oluline on kasutada tugevat parooli (minimaalne pikkus vähemalt 8 sümbolit), piirata ebaõnnestunud sisselogimiskatsete lubatud arvu ning nõuda korrapärast parooli vahetamist (nt 3 kuu tagant). Erinevates keskkondades tuleks kasutada erinevaid paroole. Kasutajatele tuleb selgitada paroolipoliitika vajalikkust ning juhendada kasutajaid sobiva turvalise parooli koostamisel (näiteks kasutada paroolisõnade asemel nö paroolilauseid, asendada paroolis teatud tähed numbritega, lisada kirjavahemärke jms).

Suurima turvalisuse tagab juurdepääsuõiguste lahendamine selliselt, et kasutajaid tuvastatakse ID-kaardi ja/või Mobiil-ID abil.

Ruumide signalisatsiooni valvekoodi (nn masterkood) tuleb hoida seifis või mõnes muus ettevõtte turvapoliitikaga määratud turvalises kohas. Turvaliselt tuleb hoida ka töötajatele väljastatud signalisatsiooni valvekoode.

Kui töötaja lahkub ettevõttest või puudub pikka aega töölt (näiteks haiguse tõttu), siis tuleb paroolid ja muud pääsuvõimalused viivitamata kehtetuks muuta.

2.5. Töötajate teadlikkus ja koolitus

Ettevõtte töötajad peavad olema teadlikud oma ülesannetest ja vastutusest. Koolitage oma töötajaid ära tundma selliseid ohte nagu (1) andmepüügi e-kirjad, (2) e-postiga saadetavad nakatatud

[9] Isikuandmete kaitse seadus § 25 lõige 2.

dokumendid ja muud failid, (3) ebaturvalisi võrgulehti külastades automaatselt levitatav pahavara, (4) teisaldatavate andmekandjate (USB mälupulgad, välised kõvakettad jms) kaudu leviv pahavara ning muud arvutite ja võrgu kasutamisest tulenevad ohud. Hoiatage töötajaid riskide eest, mis kaasnevad ettevõtte tegevust puudutava teabe avaldamisega sotsiaalvõrgustikes, veebifoorumites ja -kommentaariumites. Juhtige töötajate tähelepanu sellele, et vastava teabe avaldamine võib kaasa tuua probleeme ka juhul, kui seda tehakse näiteks pereringis või avalikus kohas kõvahäälselt arutades. Kujundage töötajates arusaam, et ettevõttele usaldatud isikuandmeid võib töötaja kasutada vaid tööalaselt.

Seadus kohustab isikuandmete töötlejat tagama oma alluvuses isikuandmeid töötlevate isikute väljaõppe isikuandmete kaitse alal.[10]

2.6. Segmenteerimine

Isikuandmetega seotud rikkumisi saab ära hoida või nende raskusastet vähendada, eraldades ja piirates juurdepääsu võrgukomponentide kaupa. Näiteks peaks veebiserver olema eraldi põhilisest failiserverist. See tähendab, et ettevõtte võrgulehe kahjustamise korral ei ole ründajal otsest juurdepääsu ettevõtte kesksele andmebaasile. Kui ettevõtte Interneti veebiserverit on tarvis ühendada lisaks ka sisevõrguga, tuleb sisevõrku üleminekut tulemüüriga kaitsta.

2.7. Seadmete tugevdamine

Eemaldage ettevõtte seadmetelt tarkvara ja teenused, mida ei kasutata. Nii mõnegi levinud tarkvara vanemate versioonide turvaprobleemid on hästi teada. Kui te sellist tarkvara ei kasuta, siis on selle eemaldamine tunduvalt lihtsam kui püüd ajakohastada.

Muutke kindlasti ära kõik tark- ja riistvara vaikeparoolid, sest need on ründajatele hästi teada.

3. Andmete turvalisus

Andmete sh isikuandmete töötlemisel tuleb tagada, et ettevõte hoiab väljaspool tööruume kasutatavates seadmetes olevaid isikuandmeid sama turvaliselt kui kontoris. Paljud isikuandmetega seotud rikkumised tulenevad seadme (nt sülearvuti, nutiseadme või USB-seadme) vargusest või kadumisest, ent alati tuleks jälgida ka e-posti või posti teel saadetavate andmete turvalisust. Varguse mõjusid saab vähendada, tagades, et seade ei sisalda isikuandmeid või et andmed sh isikuandmed on nõuetekohaselt kaitstud ja neile puudub juurdepääs.

Väljaspool tööruume isikuandmete töötlemisega seotud seadmete turvalist kasutamist on Andmekaitse Inspektsioon selgitanud juhises „Isikliku mobiilse seadme kasutamine töökeskkonnas.“

Kuidas toimida?

- piisavalt tugeva krüpteerimisega[11] saate tagada, et andmed on kättesaadavad üksnes volitatud kasutajatele. Krüpteeritud andmete avamiseks on vajalik salasõna (võti).
  - kogu kõvaketta krüpteerimine tähendab, et kõik arvutis olevad andmed krüpteeritakse;
  - faili krüpteerimine tähendab üksikute failide krüpteerimist;
  - andmeid tuleks krüpteerida ka neid teistele organisatsioonidele elektroonilise side võrgu[12] kaudu saates, näiteks e-postiga;

[10] Isikuandmete kaitse seadus § 26 lõige 3.
[11] Krüpteerimine tähendab loetaval kujul oleva informatsiooni muutmist loetamatuks.

- krüpteerimisel tuleks paroolina kasutada pikemat fraasi, mis sisaldaks nii suur- ja väiketähti, numbreid (näiteks teatud tähtede asendusena) kui ka sümboleid (nt #, &, !) ning seda tuleb hoida salajas;
- mõne tarkvara puhul on võimalik parooliga kaitsta andmete muutmist, ent see ei pruugi takistada vargal andmeid näha. Jälgige täpselt, millist kaitset oma andmete suhtes rakendate.
- enne isikuandmete edastamist kolmandatele osapooltele tuleb hinnata, kas nad on piisavalt usaldusväärsed ning rakendavad nõuetekohaseid turvameetmeid isikuandmete kaitseks. Kahtluste korral loobuge isikuandmete edastamisest või kasutage teisi privaatsust parandavaid lahendusi, näiteks andmete anonüümimine või pseudonüümimine.[13]

Lihtsaim võimalus failide lühiajaliseks krüpteerimiseks on kasutada **DigiDoc3 krüpto** tarkvara. Tegemist on ID-tarkvara osaga, mis paigaldatakse kasutaja arvutisse koos ID-tarkvara paigalduspaketiga. DigiDoc3 tarkvaraga saab näiteks krüpteerida tundliku sisuga infot, mida soovite saata e-postiga.

Oluline on meeles pidada, et salastatud info läheb kaotsi, kui krüpteerimise adressaadi ID-kaarti ei saa kasutada dekrüpteerimiseks (näiteks ID-kaart on kadunud või ID-kaardi sertifikaadid on aegunud).

- mõned mobiilsed seadmed toetavad kaugteel juurdepääsu takistamist või andmete kustutamist. See tähendab võimalust määrata kindlaks seadme asukoht ning vajaduse korral kõik andmed turvaliselt kustutada. Teenuse kasutamiseks peab seade olema **registreeritud, sisse lülitatud, ja asuma võrgu levialas.**
- edastage isikuandmeid mobiilsetele seadmetele üksnes siis, kui seda tegelikult vajate. Töö lõpetamisel kustutage seadmest andmed. Veenduge, et andmed pole näiteks kopeerimisel jäänud seadme vahemälusse.[14]

4. IT-süsteemi ajakohastamine

Selleks, et IT-seadmed ja –tarkvara toimiksid tõrgeteta ning turvaprobleeme oleks võimalik ennetada ja riske maandada, tuleb neid korrapäraselt hooldada ja uuendada. Sama kehtib turvatarkvara (nt viirustõrje ja pahavaratõrje) kohta – piisava kaitse tagamiseks on tarkvara igapäevane uuendamine hädavajalik.

Kuidas toimida?

- kontrollige, kas turvatarkvara on sisse lülitatud ja jälgib faile nii, nagu peab;
- hoidke tarkvara ajakohasena, kontrollides korrapäraselt uuenduste olemasolu ja rakendades neid. Enamikku tarkvara saab seadistada end automaatselt ajakohastama;
- kui ettevõtte infosüsteem on veidi vanem, siis tuleks kontrollida, kas selle kaitse on endiselt piisav;

---

[12] Elektroonilise side seadus § 2 punkt 8.
[13] Euroopa andmekaitseasutuste ühise töörühma arvamus nr 05/2014 anonüümimistehnikate kohta.
[14] Juhised vahemälu kustutamiseks leiate oma seadme operatsioonisüsteemi abiinfost.

- hoidke end kursis ohtudega, lugedes erialaorganisatsioonide turvalisuseteemalisi väljaandeid või võrgulehti. Näiteks infoturbe- ja IT haldusega seotud teemasid Riigi Infosüsteemi Ameti võrgulehel, tehnoloogia mõjudest inimeste privaatsusele Andmekaitse Inspektsiooni võrgulehel.

5. Probleemide jälgimine

Küberkurjategijad või pahavara võivad ettevõtte infosüsteeme märkamatult rünnata. Paljud avastavad liiga hilja, et neid on rünnatud, ehkki hoiatavad märgid olid olemas.

Kuidas toimida?

- kontrollige korrapäraselt ettevõtte turvatarkvara teateid, juurdepääsu kontroll-logisid ja muid aruandlussüsteeme, mida kasutate;
- tagage võimalus kontrollida, milline tarkvara või millised teenused ettevõtte võrgus töötavad. Te peaksite olema võimelised tuvastama, kas võrgus esineb midagi, mida seal ei peaks olema;
- käivitage korrapäraselt turvaskaneerimine ja tehke läbivusteste, et kontrollida oma infosüsteemi teadaolevate probleemide suhtes. Tagage tuvastatud probleemide lahendamine;
- kui ettevõtte tegevust reguleerivad seadused ei sätesta teisiti, tuleks andmehaldus- ja infosüsteemide logisid säilitada nii kaua, kui see on vajalik andmetöötluse eesmärkide täitmiseks.

6. Kohustuste teadvustamine

Mõnede ettevõtete kaitsetase pole piisav, sest nad ei kasuta oma olemasolevaid turvameetmeid õigesti ega suuda alati probleemi avastada. Tuleb tagada, et kõik töötajad oleksid teadlikud oma ülesannetest ja vastutusest ning teaksid, millal ja milliseid meetmeid kasutada. Samuti tuleks mõelda, milliseid meetmeid rakendada, kui ilmneb isikuandmetega seotud rikkumine.

Kuidas toimida?

- tehke endale ülevaade kõikidest oma valdkonna õiguslikest nõuetest ja headest tavadest;
- dokumenteerige oma olemasolevad kontrollimeetmed ja tehke kindlaks, millal on vaja parendusi;
- kui parendused on tehtud, siis jälgige jätkuvalt kontrollimeetmeid ja kohandage neid vajaduse korral;
- tehke kindlaks ettevõttes hoitavate isikuandmete kõik riskitegurid ning määrake, kuidas toimite isikuandmetega seotud rikkumise korral. Sel viisil saate halvima juhtumisel pehmendada tagajärgi;
- koostage töötajatele koolitusmaterjalid, et nad teaksid oma andmekaitsealast vastutust; kontrollige omandatud teadmisi;
- laske turvaeksperdil oma süsteemid üle vaadata;

Ärge unustage oma andmetest varukoopiaid teha. Varukoopiaid tuleks teha korrapäraselt ja hoida turvaliselt ning kustutada nõuetekohaselt[15], kui te neid enam ei vaja.

7. Isikuandmete minimaalsus

Vastavalt seadusele peavad isikuandmed olema täpsed ja ajakohased. Neid ei tohi hoida kauem kui vajalik.[16] Aja jooksul võib ettevõttel olla kogunenud suur hulk isikuandmeid. Mõned neist andmetest võivad olla aegunud ja ebatäpsed ning muutunud ebavajalikuks.

Kuidas toimida?

- otsustage, kas andmed on veel vajalikud. Kui jah, siis kas neid hoitakse õiges kohas;
- kui peate teatavaid andmeid arhiveerimise eesmärgil alles hoidma, aga ei pea neid pidevalt kasutama, siis paigutage need turvalisemasse kohta. See aitab ära hoida volitamata juurdepääsu;

Näiteks, töölepingu säilitamise tähtajaks sätestab seadus 10 aastat. Raamatupidamisdokumentide säilitamiskohustus on 7 aastat.

- vajadusel kasutage arhiveerimisteenust pakkuvate ettevõtete abi. Nõustamist osutavad ka Rahvusarhiiv, Riigiarhiiv;
- kui Te andmeid rohkem ei vaja, kustutage nad. Ebavajalike andmete korrapärane kustutamine peab olema töökorralduse osa. Selle toimingu turvalisuse tagamiseks võite vajada eritarkvara või nõuandeid.

Korduvkirjutatavale andmekandjale (näiteks kõvaketas, mälupulk, magnetlindid) salvestatud andmeid võib kustutada uute andmetega ülekirjutamise teel. Püsiandmekandjale (näiteks CD, DVD) salvestatud andmeid saab kustutada ainult andmekandja füüsilisel hävitamisel.

8. IT-partneri kontroll

Paljud väikeettevõtted kasutavad osade või kõikide IT-lahenduste ja turvanõuete täitmiseks koostööpartnerit (volitatud töötlejat). Üha enam kasutatakse pilvetehnoloogiaid, mille puhul tuleb väga selgelt teadvustada ohte seoses turvalisuse, läbipaistvuse (näiteks teabe puudumine isikuandmete töötlemise kohta), puudustega erinevate pilvetehnoloogiate koosvõimelisusel. Enne pilveteenuste kasutamist peab ettevõte kui isikuandmete vastutav töötleja kontrollima, kas volitatud töötleja (pilveteenuse pakkuja) töötleb ettevõtte äritegevusega seotud andmeid vähemalt sama turvaliselt, kui ettevõte seda teeks. See annab võimaluse hinnata, kas isikuandmete edastamine, töötlemine ja säilitamine pilveteenuse osutaja taristus võib seada ohtu isikute turvalisuse ja eraelu puutumatuse, seda eelkõige siis, kui tegemist on tundlike andmebaaside ja teenustega. Ettevõtja peaks valima pilveteenuse pakkuja, kes tagab Euroopa Liidu andmekaitsealaste õigusaktide järgimise ja rahvusvahelise andmeedastuse seaduslikkuse.

---

[15] Korduvkirjutatavale andmekandjale (näiteks kõvaketas, mälupulk, magnetlindid) salvestatud andmeid võib kustutada uute andmetega ülekirjutamise teel. Püsiandmekandjale (näiteks CD, DVD) salvestatud andmeid saab kustutada ainult andmekandja füüsilisel hävitamisel.

[16] Isikuandmete kaitse seadus § 6 punkt 3, 5.

Kuidas toimida?

- taotlege ettevõtte andmeid, sh isikuandmeid sisaldavate infosüsteemide, turvaauditit. See võib aidata tuvastada probleeme, mille lahendamisega saate seejärel tegeleda;
- tutvuge oma IT-valdkonna koostööpartneri turvahinnangute koopiatega;
- vajaduse korral külastage oma IT-valdkonna koostööpartneri ruume, et teha kindlaks nende vastavus Teie ootustele;
- kontrollige sõlmitud lepinguid. Need peavad olema kirjalikus vormis ning neis peab olema sätestatud, et Teie koostööpartner tegutseks üksnes Teie suuniste kohaselt ning täidaks isikuandmete kaitse seaduses sätestatud kohustusi;
- nõudke IT-koostööpartnerilt regulaarselt juurdepääsulogisid, kontrollige logisid süstemaatiliselt. Nii saate veenduda, et ei toimu volitamata isikuandmete töötlemist.
- kontrollige, kas teie koostööpartner rakendab mõnda (rahvusvaheliselt) tunnustatud infoturbestandardit (näiteks ISO 27001 „Information technology – Security techniques – Information security management systems – Requirements“).
- ärge jätke tähelepanuta IT-seadmete realiseerimist. Kui te kasutate isikuandmete kustutamiseks ja IT-seadmete utiliseerimiseks või taaskasutamiseks koostööpartnerit, siis kontrollige, kas ta teeb neid toiminguid nõuetekohaselt.

Seaduse kohaselt vastutab isikuandmete vastutav töötleja (Teie ettevõte) selle eest, et volitatud töötleja (IT- koostööpartner) täidab isikuandmete töötlemise nõudeid.[17]

[17] Isikuandmete kaitse seadus § 7 lõige 4.