ANDMEKAITSE INSPEKTSIOON

Turvaline e-pood

Juhendmaterjal e-kaupmeestele isikuandmete kaitse seaduse (IKS) ja elektroonilise side seaduse (ESS) kokkupuutealade selgitamiseks

Juhend kehtestatakse isikuandmete kaitse seaduse § 33 lõike 1 punkti 5 alusel

Kinnitatud 6.11.2014

Täiendatud 3.01.2017

Sissejuhatus

Meie igapäevaelu liigub üha enam elektroonilistesse kanalitesse. Olgu selleks sideettevõtjate iseteeninduskeskkonnad, internetipangad või inimeste terviseandmed patsiendiportaalis. Avalik sektor ja kohalikud omavalitsused peavad erinevaid registreid ja andmekogusid, millele on inimestel ja organisatsioonidel juurdepääs interneti vahendusel (näiteks äriregister, rahvastikuregister, liiklusregister, kinnistusraamat).

Suurenev kaubavalik, kulukad üüripinnad ning kaupluse alati mitte sobiv asukoht on andnud kaubandusettevõtjatele tõuke arendamaks füüsilisele poele lisaks e-poode. Tarbijatele on loodud mugav võimalus osaleda mobiilse seadmega (arvuti, nutitelefon, tahvelarvuti) ostuprotsessis.

E-poe kasutamiseks küsib e-kaubandusega tegelev ettevõtja (e-kaupmees) tarbijalt erinevaid isikuandmeid. Olgu andmed kas laua- või sülearvutis, võrguserveris, pilves, mobiilses seadmes, võrgulehel, e-posti serveris või paberkandjal – kõiki neid andmeid tuleb kaitsta. Kontakti hoidmiseks soovib e-kaupmees saata aeg-ajalt tarbijatele uudiskirju või otseturustusteavitusi.

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

Andmekaitse Inspektsioon on koostanud juhise, mis selgitab, milliseid seadustest tulenevaid nõudeid peab e-kaupmees järgima turvaliseks isikuandmete töötlemiseks e-poes. Juhise eesmärk on anda soovitusi eelkõige tarbijaga seotud turvaliseks ostutoiminguks.

Ettevõtte töökorralduse-, infoturbe- ja isikuandmete kaitse põhimõtteid selgitab inspektsioon põhjalikumalt juhises „Infoturve ja isikuandmete kaitse väikeettevõttes“.

1. Tarbija registreerimine

E-kaupmees kogub ja salvestab e-poes teenust osutades erinevaid tarbijaga seotud isikuandmeid.

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

Iga isikuandmetega tehtav toiming on isikuandmete töötlemine.[2]

E-poes on tarbijal võimalik ostu sooritada kahel moel:

1) impulssostuna – eelnev kasutajaks registreerumine pole vajalik. E-kaupmees küsib ostu vormistamiseks tarvilikud andmed enne ostu sooritamise lõppu.
2) registreerunud kasutajana – tarbija loob e-poes isikliku kasutajakonto. Konto loomiseks täidab tarbija vormi, kuhu sisestab enda kontaktandmed, näiteks e-posti aadressi, telefoni numbri, isikukoodi ja postiaadressi. Kasutajakontole juurdepääs on reeglina kasutajanime ja salasõnaga.

Pane tähele: tarbija kontaktandmed sh kasutajanimi, salasõna, e-posti aadress, postiaadress on isikuandmed.

Seadus kohustab e-kaupmeest ehk **isikuandmete töötlejat**[3] järgima isikuandmete töötlemisel seaduslikkuse, eesmärgikohasuse, minimaalsuse, kasutuse piiramise, andmete kvaliteedi, turvalisuse ja individuaalse osaluse põhimõtteid.[4]

Elektroonilises müügi- ja ostuprotsessis on ülimalt oluline järgida turvalisuse põhimõtet – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest.[5]

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 tagantjärgi tuvastada, kes millal millele juurde pääses, mida salvestas, muutis või kustutas ning kellele, millal, miks ja kuidas isikuandmeid edastati;
- tagama, et e-poe töötajatel oleks juurdepääs üksnes tööülesannete täitmiseks vajalikele andmetele ja töötlemisviisidele. Mittevajalikud juurdepääsuõigused võivad lisaks konfidentsiaalsusele põhjustada probleeme ka andmete käideldavuses[6] ning tervikluses[7];
- kujundama töökorralduse selliselt, et see võimaldaks täita andmekaitse nõudeid;
- tagama oma alluvuses isikuandmeid töötlevatele isikuile kohane väljaõpe ja teavitus turvameetmete perioodilistest uuendustest.

Turvalisuse põhimõtet tuleb samuti järgida tarbija kasutajakonto osas. Levinud turvameetmeks on salasõna nõue. Üldjuhul valib (1) tarbija salasõna ise või (2) e-pood saadab kasutajaks registreerumisel nn vaikesalasõna tarbijale e-kirjaga soovitusega salasõna hiljem ise ära muuta.

[1] IKS § 4 lõige 1.
[2] IKS § 5.
[3] IKS § 7 lõige 1.
[4] IKS § 6.
[5] IKS § 6 punkt 6.
[6] Andmete õigeaegne ja hõlbus kättesaadavus selleks volitatud isikutele.
[7] Andmete põhinemine algallikal ning veendumus, et need pole hiljem muutunud või neid pole volitusteta muudetud.

Turvalise ja nõuetele vastava salasõna kasutamine on ülimalt oluline

1.1.Tarbija valib salasõna ise

Kui e-poes on tarbijal võimalus salasõna ise valida, peaks e-kaupmees siiski andma soovitusi salasõna pikkuse ja kasutatavate sümbolite osas. Soovitused saab välja tuua näiteks eraldi avanevas infoaknas salasõna sisestuskasti kõrval. Veelgi turvalisem on lahendus, kus tarbijal ei ole e-poes võimalik teatud pikkusest lühemat salasõna sisestada.

Igal e-poe kasutajal peab olema unikaalne salasõna.

Soovituslikud nõuded salasõnale:

- salasõna peaks koosnema suur- ja väiketähtede ning numbrite kombinatsioonist;
- soovitav on salasõnas lisaks kasutada kirjavahemärke;
- salasõna ei tohiks olla koostatud vaid ühesugustest sümbolitest ega klaviatuurijärjestuses tähtedest või numbritest;
- salasõna ei tohiks olla lihtsasti tuletatav varasemalt kasutatud salasõnades, näiteks muutes salasõnas ainult ühte tähte või numbrit;
- samu salasõnu ei tohiks kasutada erinevates keskkondades;
- mida pikem salasõna, seda turvalisem. Salasõna minimaalne pikkus peaks olema vähemalt 9 sümbolit.

1.1.E-pood saadab tarbijale salasõna e-kirjaga

Sellise lahenduse korral peaks e-kaupmees samuti arvestama eelnevalt kirjeldatud soovitustega. Tarbijale peaks kehtima kohustus vaikesalasõna muutmiseks ettemääratud aja jooksul, peale mida pole vaikesalasõna kasutamine enam võimalik. See nõue on oluline, kuna valdav osa tarbijaid kasutavad senise praktika kohaselt vaikesalasõna mugavusest edasi.

Pane tähele: suurima turvalisuse tagab juurdepääsuõiguste lahendamine (e-poodi sisse logimine) selliselt, et e-poe kasutajad tuvastatakse ID-kaardi ja/või Mobiil-ID abil.

ID-kaardi ja Mobiil-ID lahenduste kohta saab lähemalt uurida AS Sertifitseerimiskeskus võrgulehelt.

2. Andmete minimaalsus

Üks isikuandmete töötlemise põhimõtteid on **minimaalsuse põhimõte** – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks.[8] E-poes on e-kaupmehe lõppeesmärk kauba toimetamine tarbijale. Sellest tulenevalt ei ole seaduspärane koguda tarbija kohta isikuandmeid, mis ei ole vajalikud eesmärgi täitmiseks.

Kui e-poes on impulssostuna võimalus tellida kaup pakiautomaati, ei tohiks pood ostu vormistamiseks küsida tarbijalt kohustuslikus korras elukohaandmeid nagu linn, tänav, majanumber.

Mainitud aadressandmed on tarvilikud juhul, kui tarbija kasutab näiteks kullerteenust.

Raamatupidamise seadus (RPS) võimaldab tehingupooleks olevale isikule, kes ei ole (1) raamatupidamiskohustuslane, (2) riigiraamatupidamiskohustuslane või (3) välismaa juriidiline isik, esitada arve, millel kirjas ainult majandustehingu toimumise aeg, majandusliku sisu kirjeldus ning majandustehingu arvnäitajad, näiteks kogus, hind ja summa.[9] Sisuliselt pole e-kaupmehel vajadust

[8] IKS § 6 punkt 3.
[9] RPS § 7 lõiked 2 ja 3.

tuvastada tarbija isikut. Kuna arvele ei pea märkima tarbija nime, siis ei ole sellise arve puhul ka alust tarbija isikuandmeid 7 aastat säilitada.[10]

3. Andmete edastamine

E-poes tuvastatakse tarbija kasutajakonto andmete põhjal. Peale kasutajaks registreerumist või olemasoleva kasutajana e-poodi sisse logimist vajutab tarbija üldjuhul nupule *Registreeru* või *Sisene*. Nüüd edastab tarbija seadme veebilehitseja tarbija isikuandmed e-poe veebiserverile. Inspektsiooni senine praktika on näidanud, et selline isikuandmete edastamine toimub levinult üle avatud internetiühenduse, mis võimaldab võrguliiklust pealt kuulata. Nii võivad tarbija isikuandmed (näiteks kasutajanimi, salasõna) sattuda soovimatult isikute kätte eesmärgiga andmeid kuritarvitada. Kuigi e-poes ei ole otseselt tarbijaga seotud tundlikku informatsiooni, võivad soovimatud isikud võõraid andmeid kasutada näiteks tarbija erinevatesse sotsiaalmeedia keskkondadesse liigipääsuks.

Pane tähele: Kasutage e-poes tarbijaga seotud isikuandmete edastamiseks krüpteerimist. Selleks sobib infoturbe protokoll TLS (*Transport Layer Security*).

4. Lepingutingimused

E-poe kasutamise eelduseks on tarbija nõustumus poe lepingutingimustega. Lepingutingimused võivad olla sõnastatud näiteks tüüptingimustena või müügi-, ostu-, kasutustingimustena. Isikuandmete töötlemise alus peab lepingus olema fikseeritud.
Lepingutingimuste oluline osa on tarbijale isikuandmete töötlemise põhimõtete selgitamine.

Lepingutingimustes peab olema kirjas:

- **kes ja milliseid isikuandmeid töötleb;**
- **mis on andmetöötluse eesmärk;**
- **kellele võidakse andmeid edastada.**

Lisaks soovitame kirja panna, kui kaua e-pood tarbija isikuandmeid säilitab[11] ning kuidas on tarbijal võimalik e-poe kasutajakonto soovi korral sulgeda (kustutada). Juhul kui isikuandmeid töödeldakse lisaks lepingu täitmise tagamisele[12] ka muul eesmärgil, peab see toimuma tarbija nõusolekul. Selline nõusolek peab olema võetud eraldi.

E-poe ülesehitus peaks olema selline, et tarbija annab nõustumuse lepingutingimustele kas (1) e-poe kasutajaks registreerumisel või (2) vahetult enne ostu vormistamist.

Vältida tuleb lahendust, kus lepingutingimused on küll e-poe võrgulehel kirjas, kuid tarbijal on võimalik e-poes oste sooritada tõendamist võimaldavat nõustumust andmata.

E-kaubanduse kauplemis- ja tarbijaõigusi on oma juhendites selgitanud E-kaubanduse Liit ning Tarbijakaitseamet.

[10] RPS § 12 kohaselt on raamatupidamisdokumentide (sh arvete) säilitamiskohustus 7 aastat.
[11] Vaata selles osas ka juhendi punkti 2.
[12] IKS § 14 lõike 1 punkti 4 kohaselt võib isikuandmeid töödelda lepingu täitmiseks ning selleks ei ole vaja eraldi nõusolekut võtta.

5. Nõusolek otseturustusteadete saatmiseks

Kuigi elektroonilise otseturustuse mõistet seaduses defineeritud ei ole, käsitletakse praktikas otseturustusena nii füüsilistele kui juriidilistele isikutele saadetavaid pakkumisi mingi toote müügiga või teenuse osutamisega seoses. Enamjaolt on otseturustuse puhul tegemist kommertsteadaannete saatmisega.

Kommertsteadaanne on igat liiki teabe edastus, mis on kavandatud otseselt või kaudselt edendama teenuse osutaja nimel kaupade või teenuste pakkumist või tõstma teenuse osutaja mainet.[13]

Kommertsteadaannete edastamise tingimused ja elektrooniliste kontaktandmete kasutamine on reguleeritud elektroonilise side seaduse §-s 103[1].

Pane tähele: e-poe uudiskiri või teavitus sooduspakkumistest on kommertsteadaanded.

Füüsilise isiku elektrooniliste kontaktandmete kasutamine otseturustuseks on lubatud üksnes tema **eelneval nõusolekul**.[14]

Nõusolek on tahteavaldus, millega tarbija (füüsiline isik) lubab oma isikuandmeid vabal tahtel töödelda. Selleks, et nõusolek oleks kehtiv, peab see olema **kirjalikku taasesitamist võimaldavas** vormis.[15]

Füüsilisest isikust tarbijal peab nõusoleku andmise ajal olema selge, kellele ja milleks ta nõusoleku annab. E-poes täidab seda nõuet näiteks võimalus märkida „linnukesega" vastav lahter. Või mõni muu infotehniline lahendus, mis võimaldab tarbijal selgelt ja üheselt aru saada nõusoleku andmisest ning mida on e-kaupmehel võimalik hiljem tõendada.

Pane tähele:

- **vaikimist või tegevusetust nõusolekuks ei loeta;**
- **nõusoleku tõendamise kohustus on isikuandmete töötlejal ehk e-kaupmehel;**
- **e-kaupmehe käitumine, kus nõusoleku lahter on e-poes juba eeltäidetud, on õigustühine.**

Kui e-kaupmees soovib saata uudiskirju jm reklaampostitusi, peab füüsilisest isikust tarbijale andma võimaluse vabatahtliku nõusoleku esitamiseks ja nõusoleku andmise üle otsustamiseks. Nõusoleku andmist või mitteandmist peab inimene saama vabalt valida.

Pane tähele:

- **kui otseturustuseks kasutatakse juriidilise isiku kontaktandmeid, siis eelneva nõusoleku omamise kohustust ei ole, kuid talle peab andma võimaluse keelata oma kontaktandmete edasine selline kasutamine;**
- **füüsilisele kui ka juriidilisele isikule tuleb anda iga kord, kui tema elektroonilisi kontaktandmeid kasutatakse otseturustuseks, selge ja arusaadav võimalus tasuta ning lihtsal viisil keelata oma kontaktandmete selline kasutamine. Isikul peab olema võimalus nimetatud õigust realiseerida elektroonilise side võrgu kaudu.[16]**

Nõusoleku- ja isikuandmete töötlemise korra näidisvorm on kirjeldatud juhise **lisas.**
Vaata ka Andmekaitse Inspektsiooni juhist „Elektrooniliste kontaktandmete kasutamine otseturustuses".

[13] Infoühiskonna teenuse seadus § 5 lõige 1.
[14] IKS § 12.
[15] IKS § 10 lõige 1 ja § 12 lõige 1, 2 ja 8.
[16] ESS § 103[1] lõige 2 ja 4.

6. Vastutus

Andmekaitse Inspektsioonil on õigus alustada e-kaupmehe suhtes **riiklikku järelevalvemenetlust** märgukirja või kaebuse alusel või omal algatusel.[17] Kui riiklik järelevalvemenetlus lõpeb e-kaupmehele ettekirjutuse tegemisega (näiteks e-kaupmees kogub tarbijatelt põhjendamatult palju isikuandmeid, nõrkade turvameetmete tõttu on tarbijate isikuandmed lekkinud või e-kaupmees saadab tarbijale ilma nõusolekuta kommertsteadaandeid), kuid e-kaupmees eirab ettekirjutust ja jätkab ebaseaduslikku tegevust, on inspektsioonil õigus kohaldada e-kaupmehe suhtes sunniraha ettekirjutuse täitmiseks. Kusjuures Andmekaitse Inspektsioon võib ettekirjutuse täitmiseks kohaldada sunniraha korduvalt. Sunniraha ülemmäär on **9600 eurot**.[18]

Inspektsioon võib lisaks alustada väärteokoosseisu tuvastamisel e-kaupmehe suhtes **väärteomenetluse.** Trahv isikuandmete töötlemise nõuete rikkumise eest on kuni **1200 eurot**, kui rikkujaks on füüsiline isik.[19] Juriidilise isiku puhul on vastav trahvisumma kuni **32000 eurot.**[20]

[17] IKS § 33 lõige 5.
[18] IKS § 40 lõige 2.
[19] IKS § 42 lõige 1.
[20] IKS § 42 lõige 2.

Lisa

Isikuandmete töötlemise kord *(näidistekst)*

□ *Olen tutvunud ja nõustun …(ettevõtja X)… e-poe kasutajatingimustega, sh kasutajatingimustes fikseeritud isikuandmete töötlemise korraga.(kasutajatingimused peaksid olema lihtsalt leitavad või hüperlingitud, et klient saaks enne ostu sooritamist nendega tutvuda)*

…(firma)… töötleb Teie isikuandmeid kooskõlas isikuandmete kaitse seaduses kehtestatud nõuetega. (kasutustingimustes peab olema välja toodud ettevõtte nimi, aadress ja kontaktandmed)

Meie ettevõtja töötleb isikuandmeid ainult Teie tellitud kauba kätte toimetamiseks (vajadusel lisada isikuandmete töötlemise eesmärke). Me ei edasta, müü ega avalikusta Teie andmeid kolmandatele osapooltele ilma Teie eelneva nõusolekuta või seaduses sätestatud juhtudel. (kui kasutatakse kullerfirmat või edastatakse andmeid partnerfirmale tuleks sellele viidata ja teha teatavaks kullerfirma/partnerfirma või nende esindajate nimed, firmade aadressid ja muud kontaktandmed[21])

Meie firma töötleb Teie: ees- ja perekonnanime, telefoninumbrit, e-maili, isikukoodi jne… (lõplik loetelu isikuandmetest mida ettevõte töötleb)

Kui olete avaldanud soovi saada meie ettevõtte uudiskirju on Teil alati õigus nendest loobuda. (kui firma tahab saata ka oma tütarettevõtete ja partnerite uudiskirju peab see olema tingimustes välja toodud ning loetelu tütarettevõtetest või koostööpartneritest)

Teil on igal ajal õigus tutvuda oma isikuandmetega ning nõuda nende andmete parandamist, sulgemist või kustutamist, va juhul, kui seadus sätestab teisiti (siin võib ka kirjeldada, kui kaua ettevõte isikuandmeid säilitab).

Kõiki isikuandmeid puudutavate küsimuste korral on Teil õigus saata meile e-kiri …(emaili aadress)… või helistada numbril …(firma infotelefon)….

[21] IKS § 7 lõige 4 ja § 12 lõige 3.

Otseturustusteadete saatmise nõusoleku vorm

Kui soovid saada meie ettevõtja toodete pakkumisi, palun täida selleks alljärgnev vorm:

Annan nõusoleku ettevõtjale X tema ja tema koostööpartnerite pakkumiste saatmiseks e-posti teel minu e-posti aadressile _____ ja lühisõnumina minu mobiiltelefoni numbrile _____.

Koostööpartnerite nimekiri on kättesaadav http://www.ettevotex.ee/partnerid.

Ettevõtja X ei edasta Sinu poolt avaldatud kontaktandmeid ettevõtja X koostööpartneritele, tütarettevõtetele, ega teistele kolmandatele isikutele, välja arvatud seaduses ette nähtud juhtudel riigiasutustele nende seadusjärgsete ülesannete täitmiseks. Kõik pakkumised edastatakse kas ettevõtja X nimel või ettevõtja X vahendusel.

Sul on õigus:

** igal ajal loobuda pakkumiste saamisest iga pakkumise juures ära näidatud lingile vajutades;*

** pöörduda ettevõtja X poole, kui Sul on küsimusi oma kontaktandmete kasutamise osas, telefoni teel 123 3210 või e-posti teel ettevotex@ettevotex.ee.*

** küsida ettevõtjalt X enda kohta käivaid andmeid, mida ettevõtja X Sinu kohta on kogunud.*

Ettevõtja X kontaktandmed: X tee 12, 12121 X alevik, X maakond; e-post: ettevotex@ettevotex.ee, telefon 123 3210.