Isikuandmete kaitsest ettevõtjale

Andres Ojaver
Isikuandmete kaitse ekspert
26. oktoober 2017

TALLINNA ÜLIKOOL

Olulised aspektid

- Eesmärk tugevdada eraisikute õigust privaatsusele
- Paljud printsiibid jäävad samaks, kuid täpsustuvad
- Ettevõtetel suurem dokumenteerimise koormus
- Andmete töötlus tuleb „kaardistada“, põhjendada, vajadusel kustutada
- Riskid muutuvad ettevõtetele kallimaks

konkreetsed muudatused määruses

- Isiku õigused täpsustuvad
- Mõjuhinnang
- Nõusolek või õigustatud huvi
- Tegevuste läbipaistvus
- Volitatud töötlejad
- Andmekaitseametnik
- Rikkumistest teavitamise kohustus
- Rangemad karistused

Isiku õiguste mõju ettevõttele

- Õigus tutvuda enda andmetega
- Õigus andmete parandamisele
- Õigus isikuandmete töötlemise piiramisele
- Andmete ülekandmise õigus (*uus õigus*)*
- Õigus andmete kustutamisele („õigus olla unustatud“)
- Õigus esitada vastuväiteid
- Automatiseeritud töötlusel põhinevate üksikotsuste tegemise vaidlustamise õigus, sealhulgas profiilianalüüs

Isiku õigus andmete ülekandmisele (portability)

- Nõusolek ja lepingu täitmine
- Mida see õigus täpsemalt hõlmab? Andmed, mille isik annab aga mitte ainult.
- Tehniliselt keerukas, arendused võivad osutuda keerukaks ja kulukaks
- Kui on ainult anonüümsed andmed, siis sellistele andmetele ülekandmise õigus ei kohaldu!

Andmekaitse mõjuhinnang

- *Privacy by design* põhimõte
- Millal mõjuhinnang läbi viia? (*art 35 (3)*)
- Mõjuhinnangu peavad tegema kõik need andmetöötlejad, kelle isikuandmete
  töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib tõenäoliselt füüsilistele isikute õigustele ja vabadustele kõrge risk.
- Samuti tuleb mõjude hindamine läbi viia ka siis, kui andmetöötleja hakkab kasutama (uut) tehnoloogiat, millega tal varem kokkupuudet pole olnud.
- AKI tõlgendusdokument ilmunud eelkonsultatsiooni põhimõtte tõlgendamiseks

Nõusolek või õigustatud huvi

Nõusolek – vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega klient avalduse vormis või selge tegevusega nõustub tema kohta käivate isikuandmete töötlemisega.

- Nõusolek peab olema konkreetne ja eraldiseisev ning vaba tahet hinnatakse selle järgi, kas teenust saab ka nõusolekuta.
- Kliendil õigus oma nõusolek igal ajal tagasi võtta
- Õigus nõuda andmete kustutamist pärast nõusoleku tagasivõtmist.

Õigustatud huvi – võib olemas olla näiteks siis, kui isik on ettevõtte klient või töötaja. Igal juhul tuleks õigustatud huvi olemasolu hoolikalt hinnata, sealhulgas seda, kas klient võib andmete kogumise ajal ja kontekstis eeldada, et isikuandmeid võidakse sellel otstarbel töödelda.

Tegevuste läbipaistvus

Määrus nõuab selget teavet ja isiku õiguste teostamise korda.

Kliendile peab olema kättesaadav teave, mis tuleb anda andmete kogumise hetkel (eesmärgid, jagamispõhimõtted, säilitusajad), samuti teavet kliendi õiguste kohta (juurdepääs, parandamine, kustutamine jne.) ning teavet selle kohta, et ettevõttepoolsete rikkumiste korral on ettevõte kohustatud sellest teavitama nii AKIt kui klienti.

Teave tuleb esitada kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades **selget ja lihtsat keelt**.

Volitatud töötlejad samuti hõlmatud

„volitatud töötleja“ – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.

Määrus tõstab volitatud töötlejate riski märgatavalt kõrgemaks. Rakendada võidakse sanktsioone, samuti isikute nõuded.

Dokumenteerimiskohustus (*Art 30*), turvastandardid (*Art 32*), mõjuhinnang (*Art 32*), andmekaitseametnik (*Art 37*), rahvusvaheline edastamine (*Ptk V*) ja koostöö AKI-ga (*Art 31*).

Kes peavad määrama andmekaitseametniku

(*art 37*)

- Avaliku sektori asutus või organ
- Erasektor, kui on täidetud järgmised tingimused…
  - Põhitegevus
  - Ulatuslik, korrapärane ja süstemaatiline jälgimine
  - andmete eriliikide ulatuslik töötlemine

Rikkumisest teavitamise kohustus

(*art 33, 34*) Järelevalveasutuse (AKI) ja isiku teavitamine isikuandmetega seotud rikkumisest

- Põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast sellest teada saamist
- Volitatud töötleja teavitab vastutavat töötlejat põhjendamatu viivituseta

Teavitus: rikkumise laad, võimaluse korral puudutatud isikute ligikaudne arv ja kirjete liigid ning ligikaudne arv. Kontaktisiku nimi ja kontaktandmed. Võimalikud tagajärjed. Võetud või kavandatud meetmeid.

- Vastutav töötleja dokumenteerib kõik rikkumised, sealhulgas rikkumise asjaolud, selle mõju ja võetud parandusmeetmed.
- Dokumendid võimaldavad järelevalveasutusel kontrollida nõuete täitmist.

Rangemad karistused

- Maksimummäärad on seatud kõrgeks põhjusel, et reeglitele mittevastavust ei kirjutataks äriplaani sisse.
- Soovitakse tähtsustada eraisiku õigust privaatsusele digitaalses suurkorporatsioonide ühiskonnas.
- Sanktsioneerimine vajab siseriiklikke rakendusakte
- Maksimummäärad

EHK SIIS...

kas:

- klientide kohta käivad isikuandmed on hoitud turvaliselt;
- kliendile saab need vajadusel kättesaadavaks teha;
- kliendile saab need vajadusel ülekantavaks teha/vastu võtta;
- kõiki andmeid on vaja ja millal kustuvad mittevajalikud andmed;
- teate, kellega andmeid jagate ja saate seda kliendiga jagada;
- olete dokumenteerinud andmete töötlemise põhimõtted;
- olete neid põhimõtteid ka tutvustanud;
- olete läbi mõtelnud, kuidas toimida kui midagi juhtub;
- suudate uued nõuded pöörata konkurentsieeliseks?

andres.ojaver@gmail.com

Isikuandmete kaitse konverents

Toimumisaeg: 1. märtsil 2018

Registreerimine: alates 1. detsember 2017

Asukoht: Hotell Euroopa, paadi 5 Tallinn

https://www.conference-expert.eu/et/konverentsid-%C3%BCritused-hetkel-t%C3%B6%C3%B6s