Isikuandmete töötlemise turvariskid

Mihkel Miidla

Oliver Kuusk

Liisa Maria Kuuskmaa

Veebiseminar
01.02.2022

Isikuandmete töötlemise turvariskid

10:00 Advokaadi vaade andmetöötluse turvalisusele: rikkumiste statistika ning andmeturbega seotud riskid ja tagajärjed

Soraineni partner Mihkel Miidla

10:25 Vastuolu isikuandmete töötluse reeglite ja tehnoloogia kiire arengu vahel masinõppe näitel

Soraineni advokaat Oliver Kuusk

10:45 Kümme nõuannet andmelekete riskide maandamiseks ja võimalike tagajärgede leevendamiseks

Soraineni advokaat Liisa Maria Kuuskmaa

Advokaadi vaade andmetöötluse turvalisusele

SORAINEN

Mihkel Miidla
Tallinn

01.02.2022

Trendid

- Rikkumisteadete arv kasvavas trendis
- Balti riikides andmekaitseasutused teevad tihedamalt koostööd
- Võrreldes teiste EL riikidega, on siin piirkonnas suur kasvupotentsiaal trahvide suurenemiseks

- *Schrems II* järellainetus
  - Vanad mudellepingud asendada uutega hiljemalt 27.12.2022
  - Mudellepingutele tuginemine ja USA-sse andmete edastamine jätkuvalt problemaatiline

- Uute tehnoloogiate järjest suurem sõltuvus järjest suurematest andmemahtudest. Keerukuse kasv.
- ePrivacy (küpsised, *adtech*)
- Mitte ainult EL ja GDPR – andmekaitse alased õigusaktid nüüd ka paljudes teistes riikides

Rikkumiste statistika

Alates GDPR-i kohalduma hakkamisest 25.05.2018

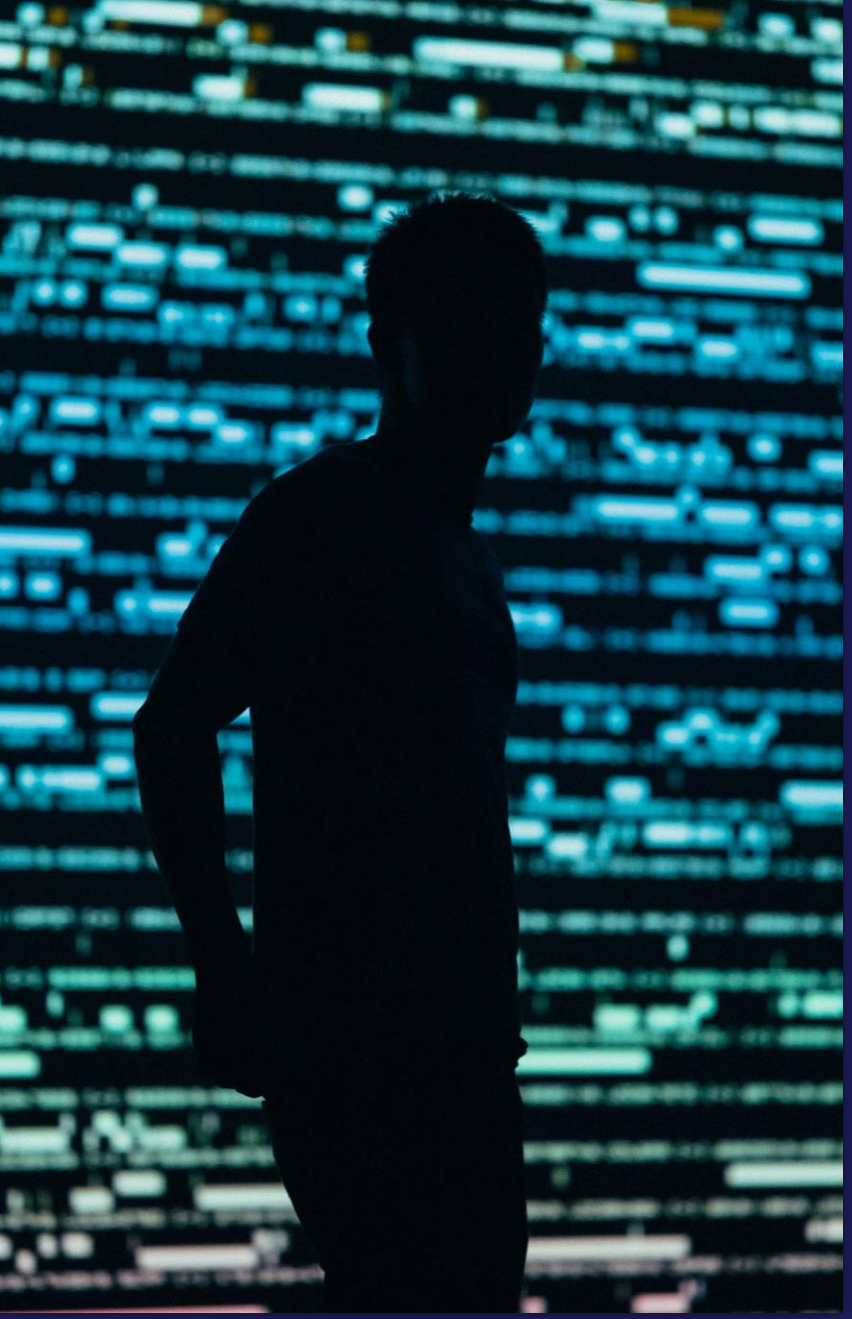
- EE
  - rikkumisteateid: 500+
  - trahvid (sh sunniraha hoiatused/määramised)
    - Suurim: 25 000 EUR *Olerex*
    - Kokku: ~85 000 EUR (sellest vaid 836 EUR väärteotrahvid)
- EL
  - EL suurimad
    - 746 MEUR (LU) *Amazon**
    - 225 MEUR (IE) *WhatsApp**
    - 90 MEUR (FR) *Google Ireland**
  - EL rikkumisteated
    - DE – 106 000+
    - NL – 92 000+
    - LT – 650+
    - LV – 360+

**pole veel lõplikud – edasi kaevatud või edasikaevatavad*

Riskid (andmesubjektile)

- Andmekaitses vaadatakse riske **andmesubjekti vaatest**
- Risk = Tagajärje raskus ja selle tõenäosus
  - Andmete liigid
  - Andmesubjektide kategooria
  - Töötlemise ulatus
  - Küberohtude muutuv maastik
  - jm

- Kasutusele võetavad organisatsioonilised ja tehnilised turvameetmed peaksid vastama asjakohasele riskitasemele (eesmärk on risk maandada)
- Riskitasemest võivad sõltuda ka muud kohustused (nt otsus kas teavitada andmesubjekte isikuandmetega seotud rikkumisest)



Tagajärjed (vastutavale töötlejale)

- Usalduse kaotus
- Mainekahju
- Talentide kadu
- Andmekadu
- Rahaline mõju (käibe vähenemine, täiendavad kulud jm)
- **Õiguslikud tagajärjed**
  - Andmesubjektide taotlused
  - Teavitamiskohustused
  - Järelevalvemenetlus
  - Trahvid/sanktsioonid
  - Tsiviilvastutus
    - Koostööpartnerite ees
    - Andmesubjektide ees

Vastuolu isikuandmete töötlemise reeglite ja tehnoloogia kiire arengu vahel masinõppe näitel

SORAINEN

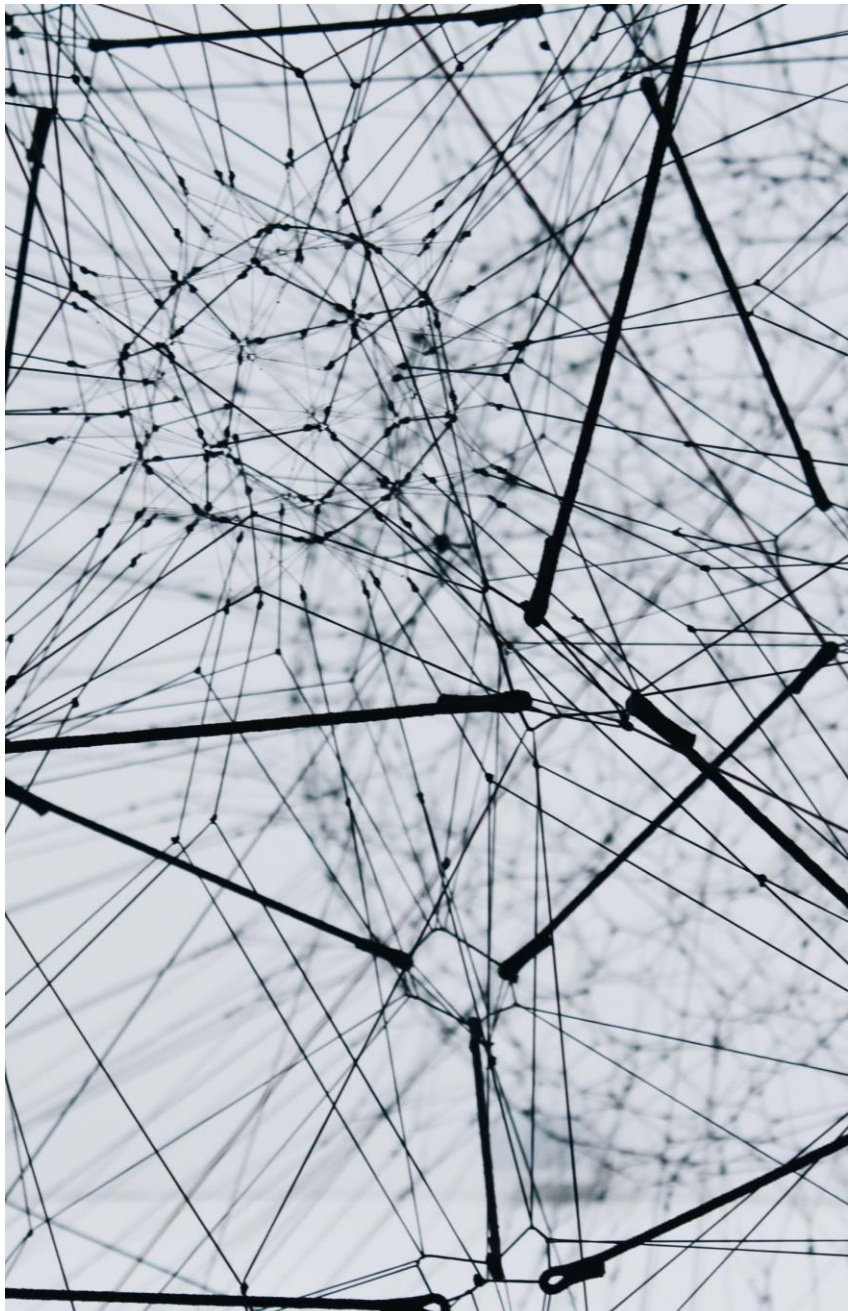
Oliver Kuusk
Advokaat

1.02.2022

Masinõpe? Isikuandmete töötlemise reeglid?

- Masinõppe puhul loob arvuti ise algoritmi, mis eraldab andmetest vajaliku info

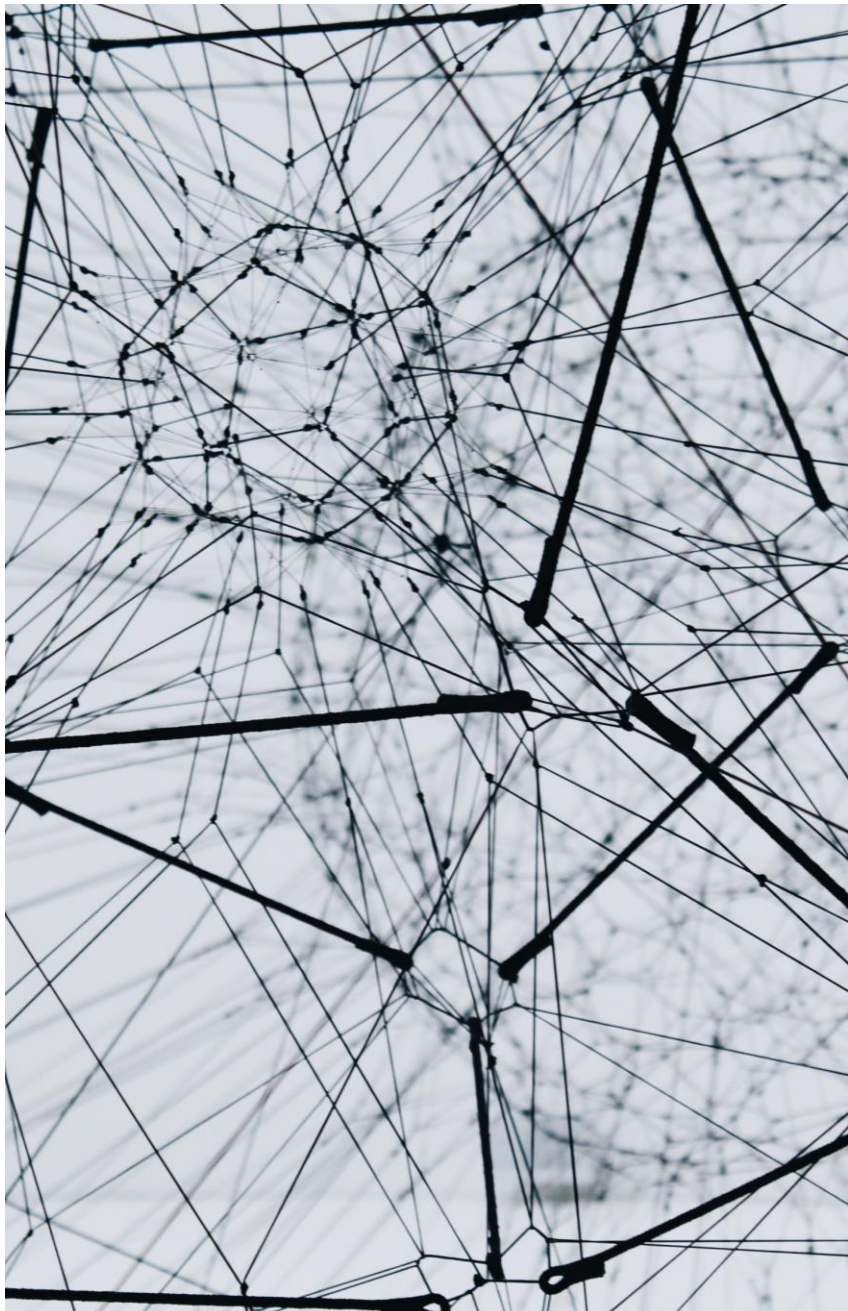
- Masinõpe
  - Vaja suurt hulka andmeid (*big data*)
  - Eesmärk või tulemuse saavutamise viis pole alati selge (*black box*)

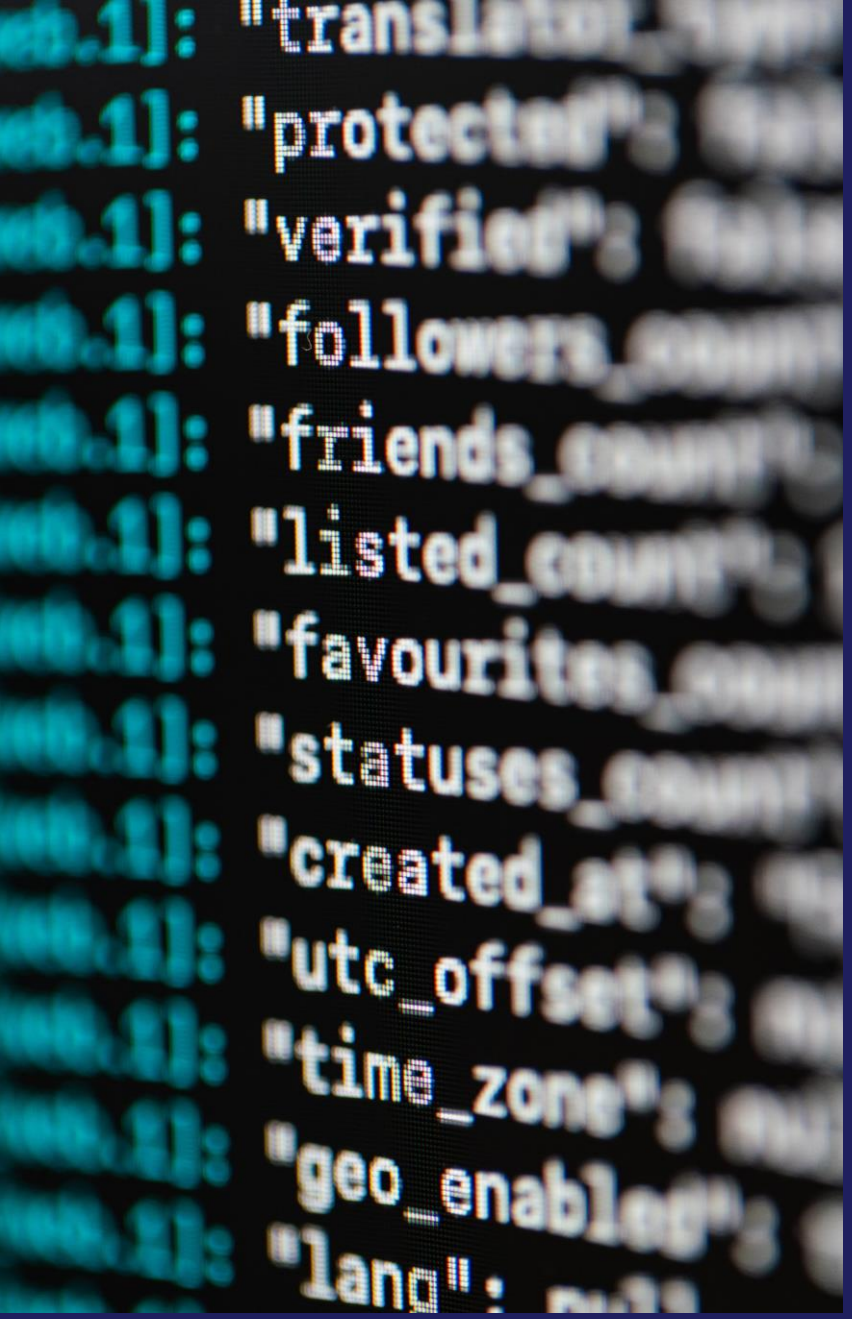


Masinõpe? Isikuandmete töötlemise reeglid?

- Isikuandmete töötlemise reeglid
  - Tehnoloogia kiire areng
  - „Vaja tugevat ja ühtsemat andmekaitseraamistikku /.../, mis võimaldab digitaalsel majandusel areneda kogu siseturu ulatuses“

- Isikuandmete töötlemise reeglid takistavad masinõpet ja tehnoloogia arengut?

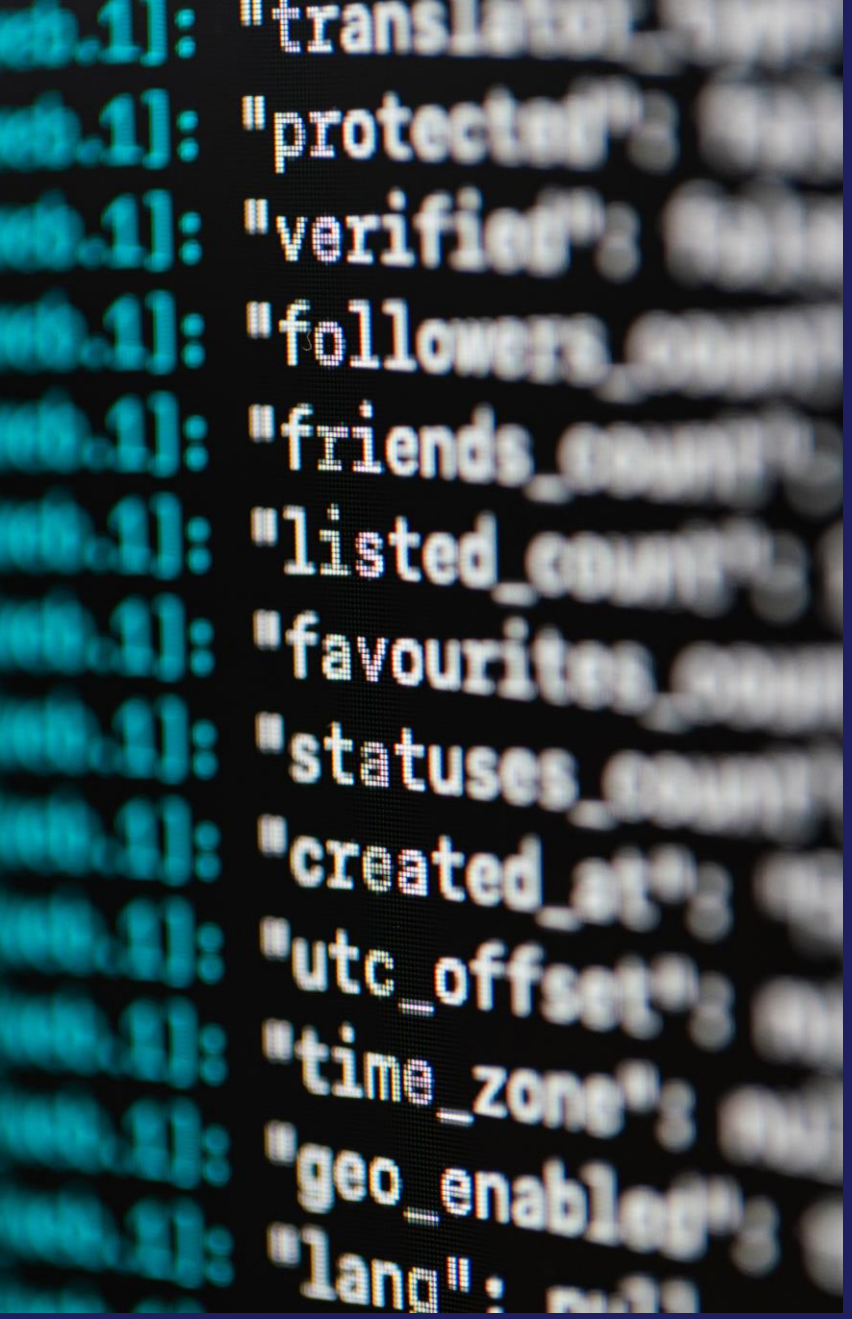




Eesmärgi piirang

- Isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid **ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus** (GDPR art 5 (1) b))

- Masinõpe
  - Eesmärk pole alati selge



Eesmärgi piirang

- Lahendus?
  - 1) Vastuolu hindamine
    - Mõistlikud ootused
    - Töötlemise tagajärjed andmesubjektile
  - 2) Statistiline eesmärk + kaitsemeetmed (nt pseudonüümid)
    - Ei tohi kasutada konkreetset isikut puudutava otsuse jaoks

Võimalikult väheste andmete kogumine

- Isikuandmed on asjakohased, olulised ja **piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt** (GDPR art 5 (1) c))

- Masinõpe
  - Vaja suurt hulka andmeid (*big data*)

Võimalikult väheste andmete kogumine

- Lahendus?
  1) Muuta andmed vähem „isikuandmeteks“
     - Pseudonüümid
     - Anonüümne teave
  2) Proportsionaalsus arvestades töötlemise kasu
     - Töötlemisest tulenev kasu *vs* riskid andmesubjektile
     - Pseudonüümid + asjakohased kaitsemeetmed

Praktikas

- Masinõpet kasutatakse võrguliikluse logifailide analüüsimisel, et tuvastada ja ennetada võimalikke küberrünnakuid.
  - Eesmärk: tagada isikuandmete konfidentsiaalsus ja terviklikkus

Läbipaistvus

- *Ex-ante*: töötlemine on seaduslik, õiglane ja **andmesubjektile läbipaistev** (GDPR art 5 (1) a))
  - Kuidas ja mis eesmärkidel
  - Selges ja arusaadavas sõnastuses
- *Ex-post*: automatiseeritud otsuste puhul õigus inimese sekkumisele (GDPR art 22 (2))
  - Õigus saada selgitust otsuse kohta
  - Sisuline teave kasutatava loogika kohta

- Masinõpe
  - Eesmärk või **tulemuse saavutamise viis pole alati selge**
  - Nn *black box* süsteemid

Läbipaistvus

- Lahendus?

  1) *Ex-ante* teavitamise kohustust pole, kui see on võimatu, nõuab ebaproportsionaalseid pingutusi või kahjustab töötlemise eesmärki (GDPR art 14 (5) b))
     - Tehnilised ja korralduslikud kaitsemeetmed

  2) XAI – *explainable AI*
     1) sisendandmed
     2) andmete hindamine
     3) eesmärgiks võetud otsus ja otsuse tagajärjed

Praktikas

- Krediidiriski hindamisel tehakse automatiseeritud otsuseid laenutaotleja laenukõlblikkuse osas.
  - Seletatav:
    1) sisendandmed: vanus, sissetulek, vara
    2) hinnatavad väärtused: künnis, mida sisendandmed peavad ületama
    3) otsuse eesmärk: laenukõlblikkus

Suur pilt ja kokkuvõte

- Vastuolud ei välista masinõppe rakendamist
- Regulatsioon
  - Tehnoloogianeutraalne
  - Paindlik

Kümme nõuannet andmelekete riskide maandamiseks ja võimalike tagajärgede leevendamiseks

SORAINEN

Liisa Maria Kuuskmaa
Advokaat

01.02.2022

Andmeleke

- **GDPR artikkel 4, punkt 12**

„isikuandmetega seotud rikkumine“ – turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu;

Konfidentsiaalsusega seotud rikkumine (*Confidentility breach)*

Isikuandmete loata või juhuslik avalikustamine või neile juurdepääs

Terviklusega seotud rikkumine (*Integrity breach)*

Isikuandmete loata või juhuslik muutmine

Kättesaadavusega seotud rikkumine (*Availability breach*)

Isikuandmetele juurdepääsu juhuslik või loata kaotsiminek või hävitamine

Andmelekke tagajärjed vastutavale töötlejale

- Sanktsioonid
  - Trahv kuni 10 000 000 või kuni 2% käibest
- Järelevalvemenetlused, võimalikud parandusmeetmete võtmise kohustused
- Nõuded
  - Andmesubjektidelt
  - Lepingupartneritelt
- Mainekahju ja usalduse kaotus
- Andmekadu = mõju äritegevusele

Riskipõhine lähenemine

GDPR artikkel 32

1. Võttes arvesse **teaduse ja tehnoloogia viimast arengut** ja rakendamise **kulusid** ning arvestades isikuandmete töötlemise **laadi, ulatust, konteksti ja eesmärke**, samuti erineva tõenäosuse ja suurusega **ohte füüsiliste isikute õigustele ja vabadustele**, rakendavad vastutav töötleja ja volitatud töötleja **ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid**, hõlmates muu hulgas vastavalt vajadusele järgmist:

a) isikuandmete pseudonümiseerimine ja krüpteerimine;

b) võime tagada isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus;

c) võime taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral;

d) tehniliste ja korralduslike meetmete tõhususe korrapärase testimise ja hindamise kord isikuandmete töötlemise turvalisuse tagamiseks.

2. Vajaliku turvalisuse taseme hindamisel **võetakse eelkõige arvesse isikuandmete töötlemisest tulenevaid ohte, eelkõige edastatavate, salvestatavate või muul viisil töödeldavate isikuandmete juhuslikku või ebaseaduslikku hävitamist, kaotsiminekut, muutmist ja loata avalikustamist või neile juurdepääsu**.

Teavitamise kohustus

Järelevalveasutuse teavitamine

- Põhjendamatu viivituseta ja võimaluse korral 72 h jooksul alates teada saamisest
- Vajadusel järk-järguline teavitamine
- Ei pea teavitama juhul, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele

Andmesubjektide teavitamine

- Vajalik, kui rikkumine kujutab endast tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele
- Ei ole vajalik, kui:
  - On kehtestatud kaitsemeetmeid, mis muudavad andmed juurdepääsuõiguseta isikutele loetamatuks (nt krüpteerimine)
  - On võetud hilisemad meetmed, et maandada suure ohu tekke tõenäosus
  - Nõuaks ebaproportsionaalseid jõupingutusi – sel juhul või teha avaliku teadaande.

10 nõuannet riskide maandamiseks ja tagajärgede leevendamiseks

1. Kaardista andmetöötlustoimingud ja riskid.
2. Määra turvaintsidentidega tegelemise eest vastutav isik.
3. Korrasta tehnilised turvameetmed.
4. Loo ettevõttesisesed protseduurireeglid.
5. Koolita töötajaid.
6. Hinda koostööpartnerite *compliance*'it.
7. Korrasta lepingud.
8. Dokumenteeri rikkumine ja sellega seoses võetud meetmed.
9. Vajadusel teavita lepingupartnerit rikkumisest.
10. Vajadusel teavita järelevalveasutust (ja andmesubjekte) rikkumisest.

Võtke meiega ühendust!

mihkel.miidla@sorainen.com

liisa.kuuskmaa@sorainen.com

oliver.kuusk@sorainen.com