# Ärihommik „Andmed ja küberturvalisus – uued nõuded, kõrgemad trahvid ja riskide juhtimise võimalused”

F-hoone 01.04.2025

SORAINEN

# Kava

9.30 Avasõnad
Mihkel Miidla, Soraineni andmekaitse ja IT-õiguse valdkonna juht, vandeadvokaat

9.35 Kas Eestis on oodata hüppelist andmekaitsetrahvide suurenemist?
Kirsika Kuutma, Andmekaitse Inspektsiooni järelevalve valdkonna jurist ja väärteomenetluse teemajuht

10.05 Küberintsidentide ja andmelekete juhtimine GDPR-i ja uue küberturvalisuse õiguse raamistikus
Oliver Kuusk, Soraineni andmekaitse- ja IT-õiguse ekspert, vandeadvokaat

10.25 Toimus andmeleke – kas peame nüüd maksma sadades tuhandetes kahjuhüvitisi?
Liisa Maria Kuuskmaa, Soraineni andmekaitse- ja IT-õiguse ekspert, vandeadvokaat

10.45 Kohvi- ja suhtluspaus

11.15 EL-i uue andmemääruse rakendamine Eestis: kus me täna oleme ja mida on oodata seadusandjalt?
Stina Avvo, Justiits- ja Digiministeeriumi IT-õiguse talituse juhataja

11.40 Tarneahela juhtimine andmekaitse ja küberturvalisuse vaatest – milleks kohustab GDPR ja uued küberturvalisuse õigusaktid?
Mihkel Miidla, Soraineni andmekaitse ja IT-õiguse valdkonna juht, vandeadvokaat

12.00 Küberkindlustusest ja kindlustusjuhtumi haldamisest
Keio Kärdla, Howden Kindlustusmaakler OÜ, küberkindlustuse spetsialist
Oliver Ämarik, Soraineni kindlustusõiguse ekspert, advokaat

12.25 Lõpusõnad
Mihkel Miidla

SORAINEN 30

# Küberintsidentide ja andmelekete juhtimine GDPR-i ja uue küberturvalisuse õiguse raamistikus

Oliver Kuusk

Vandeadvokaat

SORAINEN 30

**From:** DocuSign Info <notificationsrelyadmin@bankmenia.org>
**To:** Oliver Kuusk | Sorainen <oliver.kuusk@sorainen.com>
**Subject:** Review & Sign The Document Shared By DocuSign!!

# DocuSign


Recipient: oliver.kuusk@sorainen.com

Please DocuSign Payout Ref – AB0955379.pdf

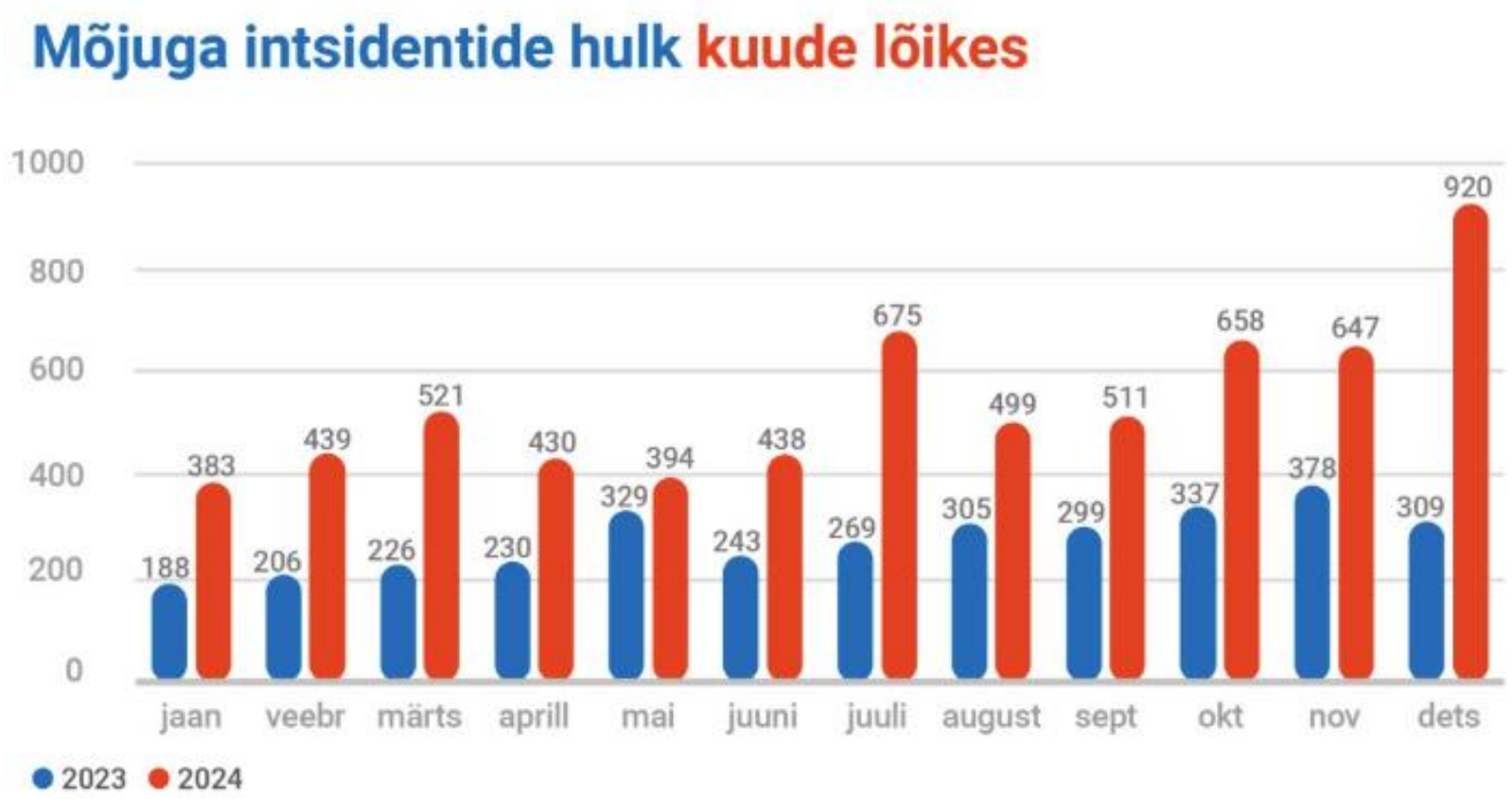
All parties have completed signature(s)

Click on the button above to review and electronically sign the document.

No hard copy is required when DocuSign is utilized.

# Küberintsidentide kasvav trend

- RIA küberturvalisuse aastaraamat 2025
  - 2023. aastal 3314 mõjuga intsidenti, 2024. aastal 6515



# GDPR ja NIS2

- **NIS2 direktiiv:** tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus
- Asendab senise NIS (NIS1) direktiivi
- Siseriiklikku õigusesse ülevõtmine hiljemalt 17.10.2024

| Aspekt | NIS2 direktiiv | Isikuandmete kaitse üldmäärus (GDPR) |
|---|---|---|
| Põhifookus | Võrgu- ja infosüsteemide turvalisus | Isikuandmete kaitse |
| Isikuline kohaldamisala | Oluline infrastruktuur ja sektorid (energeetika, transport, tervishoid, jne) | Isikuandmete töötlejad |
| Territoriaalne kohaldamisala | Euroopa Liidu territooriumil teenuseid osutavad ettevõtted | Euroopa Liidu andmesubjektide isikuandmete töötlejad, sõltumata asukohast |
| Meetmed | Riskijuhtimismeetmed, koolituskohustus, juhtorgani vastutus, **küberintsidentide teavitamiskohustus** | Töötlemise põhimõtted ja seaduslikkus, andmesubjekti õigused, **isikuandmetega seotud rikkumiste teavitamiskohustus** |

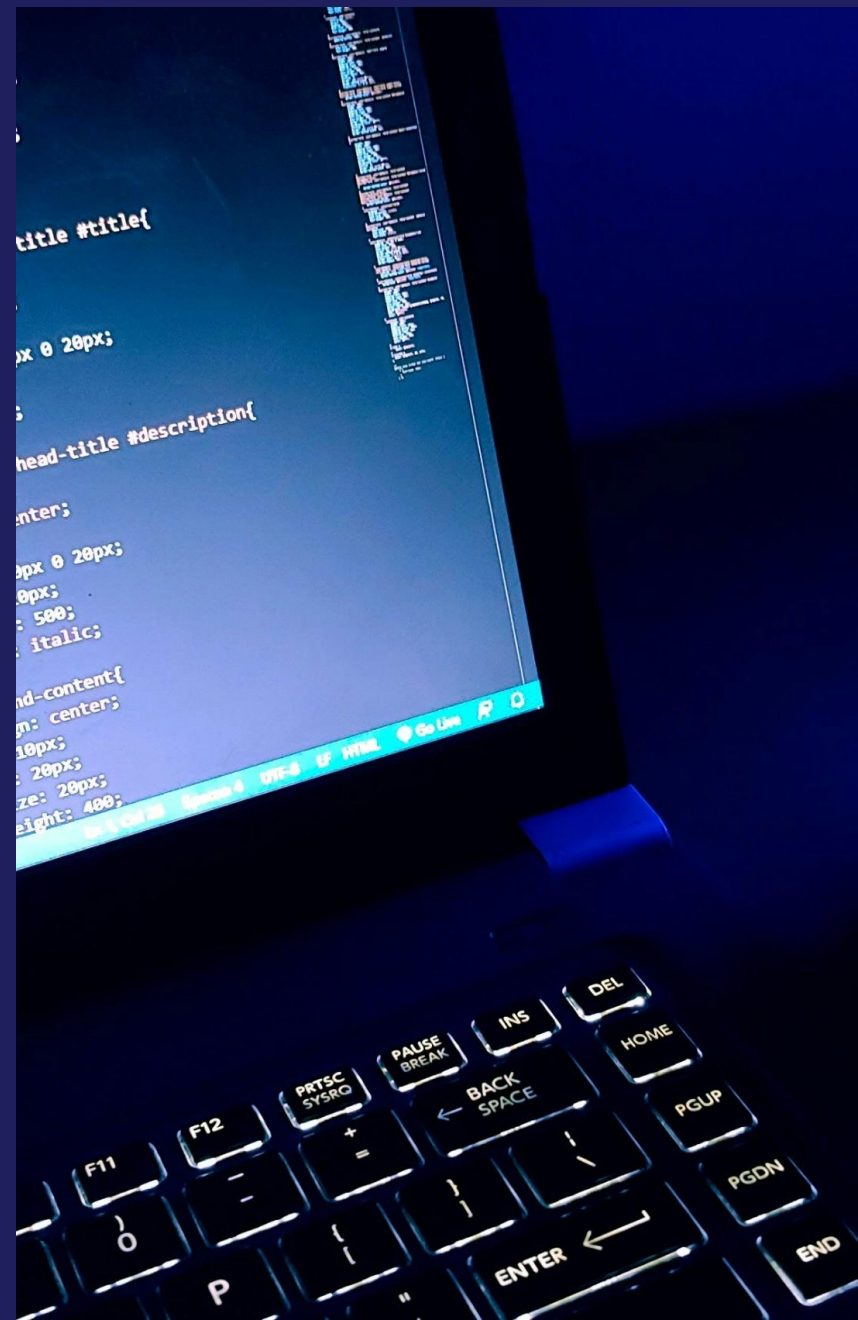
# Kas NIS2 kohaldub?

- **Elutähtsad üksused**
  - Proaktiivne järelevalve *(ex ante & ex post)*
- **Olulised üksused**
  - Reaktiivne järelevalve *(ex post)*

Liigitus sõltub üldjuhul üksuse suurusest


# Kas NIS2 kohaldub?

- Kokku ca 5500 subjekti:
  - Olemasolevaid 3537
  - Uusi ca 2000
- RIA tuvastab elutähtsad ja olulised üksused (tähtaeg 17.04.2025)

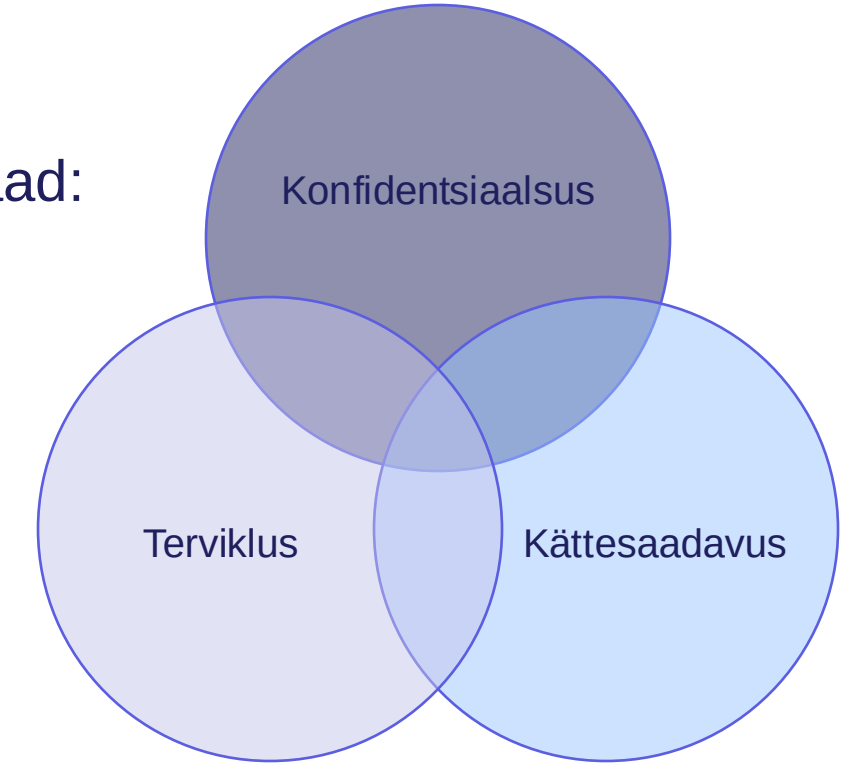


# Andmeleke ja küberintsident

**GDPR:** *turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku* ***hävitamise***, ***kaotsimineku***, ***muutmise*** *või loata* ***avalikustamise*** *või neile* ***juurdepääsu***

**NIS2**: *sündmus, mis kahjustab salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste* ***kättesaadavust***, ***autentsust***, ***terviklust*** *või* ***konfidentsiaalsust***

CIA triaad:



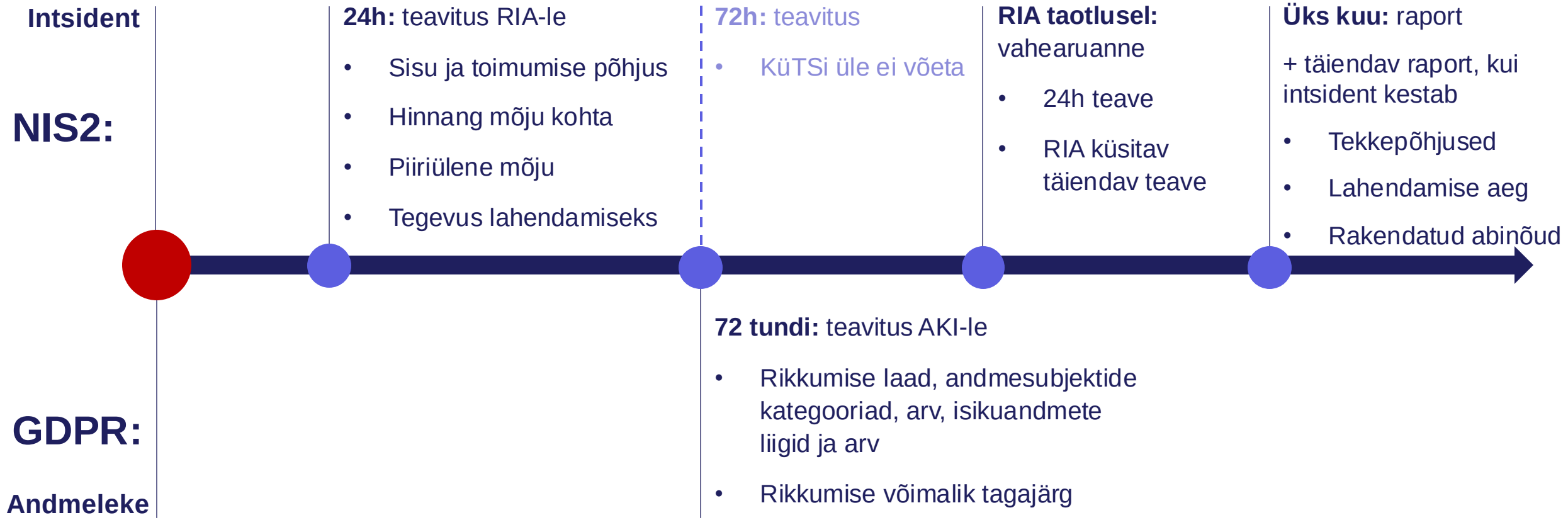
## GDPR: teavitamiskohustus

- Kõik isikuandmetega seotud rikkumised, v.a. kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele

## NIS2: teavitamiskohustus

- Oluline mõju:
  - *põhjustanud või võib põhjustada asjaomase üksuse teenuste osutamisel tõsiseid tegevushäireid või rahalist kahju;*
  - *mõjutanud või võib mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset materiaalset või mittevaralist kahju.*
- KüTS täpsemad kriteeriumid

# Teavitamiskohustused

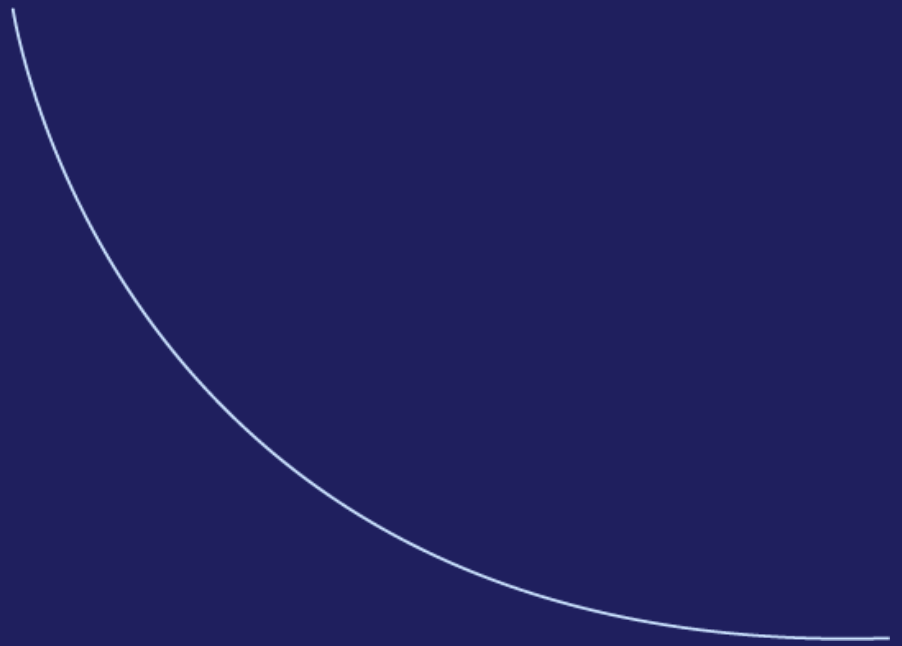



**+ DORA:** 24h+72h+1kuu

**+ Tehisintellektimäärus:** viivitamatult, hiljemalt 15 päeva jooksul

**+ Jne**

# Subjektide teavitamine

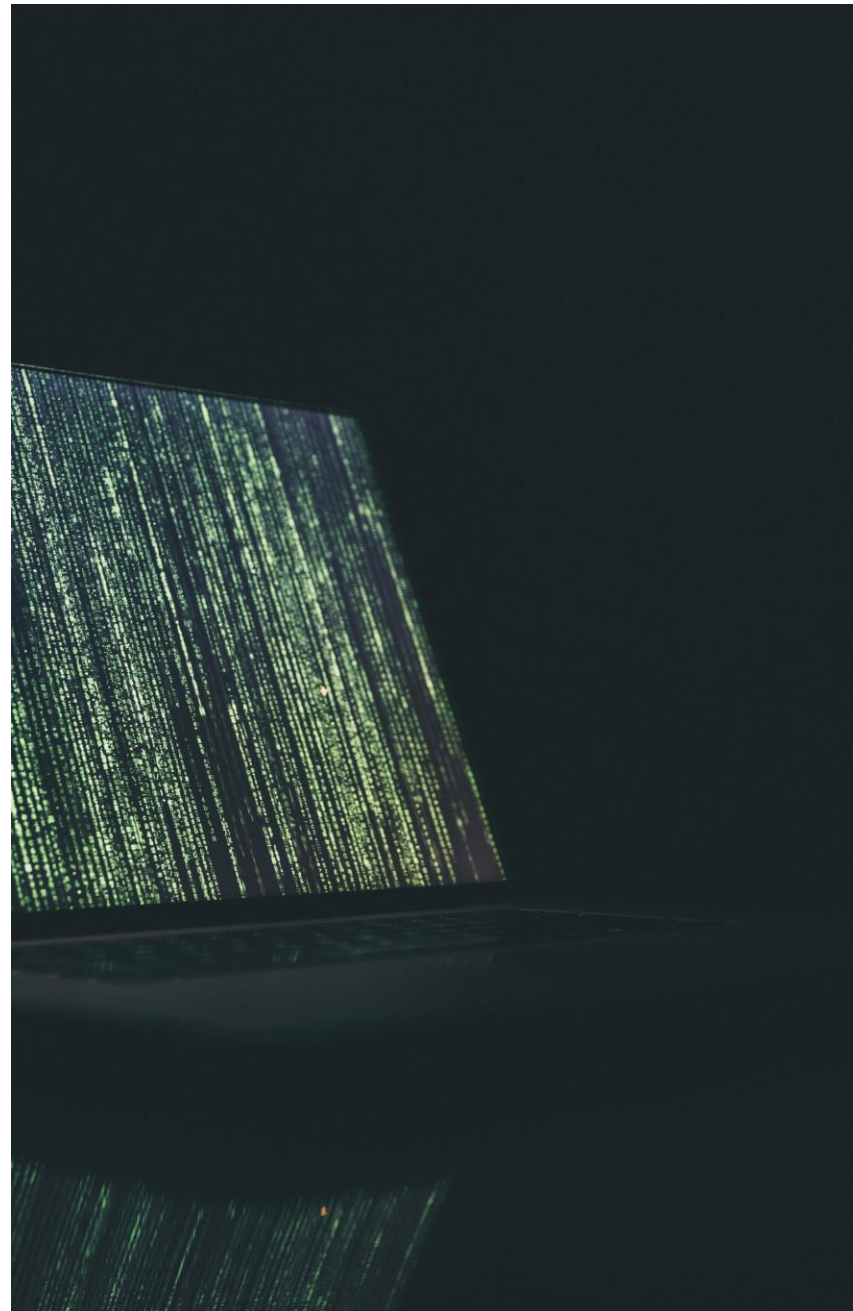


- **GDPR**: Kohustus teavitada andmesubjekti põhjendamatu viivituseta, kui rikkumine kujutab endast tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele
- **NIS2**: Kohustus teavitada mõistliku aja jooksul isikut, keda olulise mõjuga küberintsident või oluline küberoht võib mõjutada, või avalikkust, kui mõjutatud isikuid ei ole võimalik eraldi teavitada.

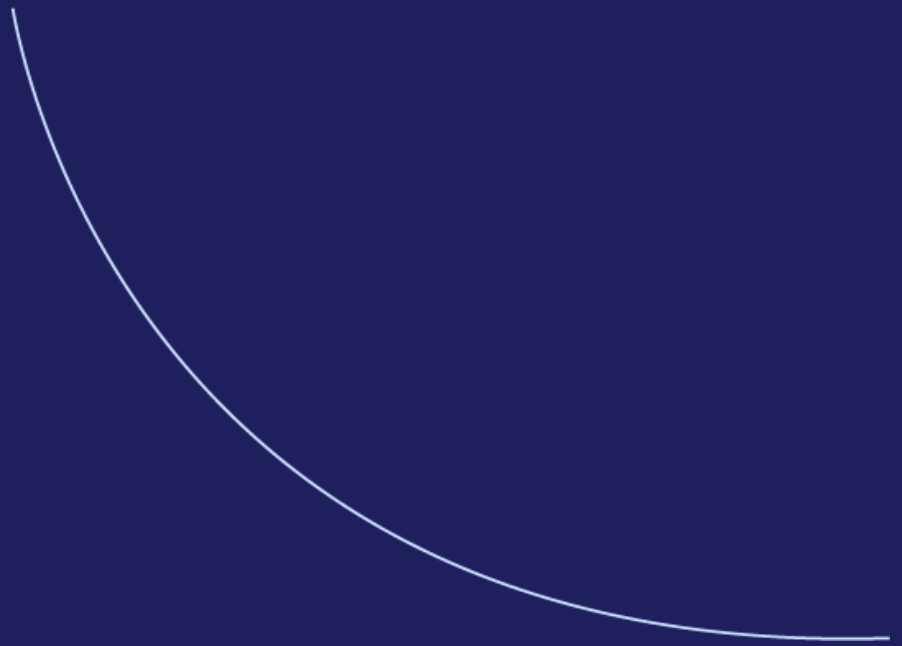
# NIS2 kohustuslikud meetmed & mõju

- Juhtidele selge vastutus
  - Juhtorganitele selged kohustused rakendada riskijuhtimismeetmeid, järgida nende rakendamist
  - Koolituskohustus
  - Juhtorgani vastutus

- Turvameetmed: asjakohased ja proportsionaalsed tehnilised, tegevuslikud ja korralduslikud riskijuhtimismeetmed
  - Küberintsidentide avastamise ja halduse protseduurid



# Kõige olulisem



1) Kas oled NIS2 skoobis
2) Lühikesed teavitamise tähtajad (24h + 72h)
3) Intsidentide avastamise ja halduse protseduurid
4) Juhtorgani vastutus

Aitäh!

Võta ühendust:
oliver.kuusk@sorainen.com

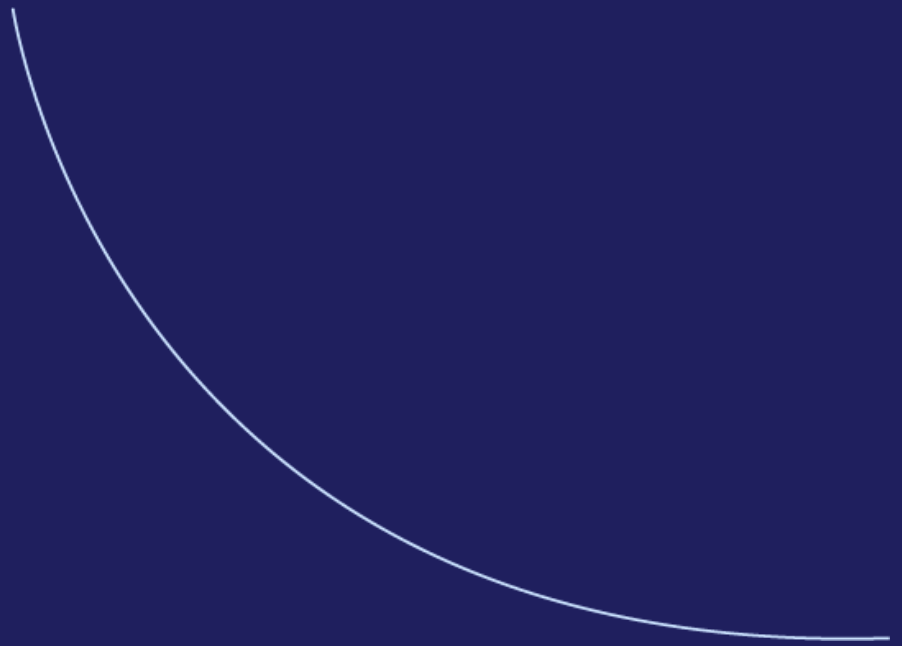
SORAINEN 30

# Toimus andmeleke – kas peame nüüd maksma sadades tuhandetes kahjuhüvitisi?

Liisa Maria Kuuskmaa
Vandeadvokaat

SORAINEN 30

# Teemad



- IKÜM/GDPR artikkel 82 ja selle rakendamise praktika Euroopa kohtus
- Andmesubjektide kahjunõuded Eesti kohtupraktikas
- Andmesubjektide kollektiivsed esindushagid

# Artikkel 82 – õigus hüvitisele ja vastutus

1. Igal isikul, kes on kandnud käesoleva määruse rikkumise tulemusel materiaalset või mittemateriaalset kahju, on õigus saada vastutavalt töötlejalt või volitatud töötlejalt hüvitist tekitatud kahju eest.
2. Kõnealuse töötlemisega seotud vastutav töötleja vastutab kahju eest, mis on tekkinud sellise töötlemise tulemusel, millega rikutakse käesolevat määrust. Volitatud töötleja vastutab töötlemise käigus tekitatud kahju eest ainult siis, kui ta ei ole täitnud käesoleva määruse nõudeid, mis on suunatud konkreetselt volitatud töötlejatele, või kui ta pole järginud vastutava töötleja seaduslikke juhiseid või on tegutsenud nende vastaselt.
3. Vastutav töötleja või volitatud töötleja vabastatakse vastutusest lõike 2 kohaselt, kui ta tõendab, et ei ole mingil viisil vastutav kahju põhjustanud sündmuse eest.
4. Kui sama töötlemisega on seotud rohkem kui üks vastutav töötleja või volitatud töötleja või nii vastutav kui ka volitatud töötleja ning nad on lõigete 2 ja 3 kohaselt vastutavad töötlemisega tekitatud kahju eest, võetakse vastutav töötleja või volitatud töötleja vastutusele kogu kahju eest, et tagada andmesubjektile tõhus hüvitamine.
5. Kui vastutav töötleja või volitatud töötleja on tekitatud kahju kooskõlas lõikega 4 täielikult hüvitanud, on sellel vastutaval töötlejal või volitatud töötlejal õigus nõuda teistelt sama töötlemisega seotud vastutavatelt või volitatud töötlejatelt tagasi see hüvitise osa, mis vastab lõikes 2 sätestatud tingimuste kohaselt sellele osale kahjust, mille eest nemad vastutavad.
6. /.../

# 4. mai 2023: *UI v Österreichische Post AG* (C-300/21)

Pelgalt IKÜM-i sätete rikkumisest ei piisa, et tekiks õigus hüvitisele.

Artikkel 82 kohase kahjunõude eeldused:

(i) isikuandmete töötlemine on vastuolus IKÜM-i nõuetega,

(ii) andmesubjektile on tekkinud kahju,

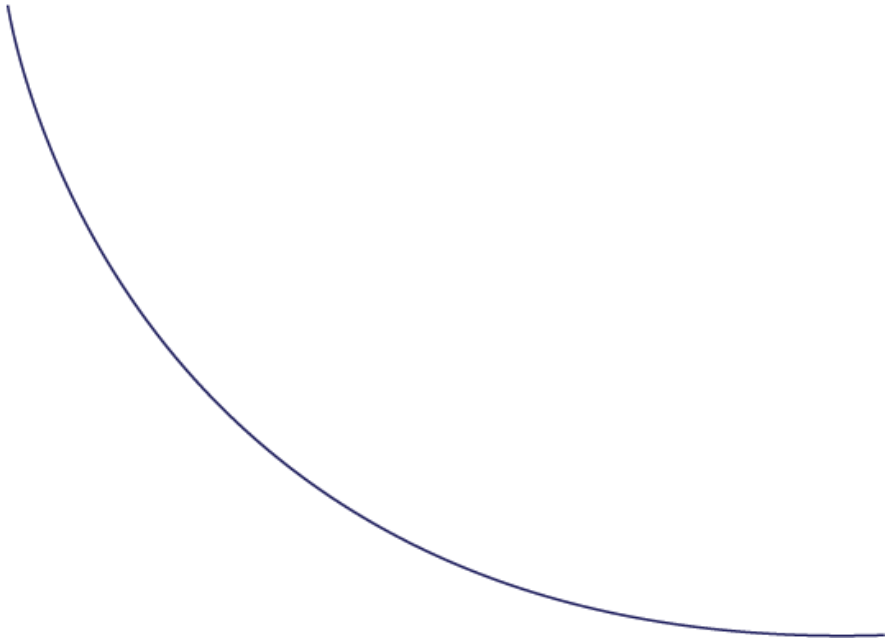
(iii) ebaseadusliku töötlemise ja tekkinud kahju vahel on põhjuslik seos.

Andmesubjektile tekkinud kahju ei pea olema teatud raskusastmega (puuduvad *de minimis* kriteeriumid).

Andmesubjekt peab tõendama, et negatiivsed tagajärjed kvalifitseeruvad mittevaraliseks kahjuks.

Kahjuhüvitise suuruse kindlaksmääramisel kohaldatakse riigisiseseid õigusnorme, arvestades EL-i õiguse võrdväärsuse ja tõhususe põhimõtetega.

# Hirm andmete väärkasutuse ees = mittevaraline kahju?



14.12.2023, C-456/22 (*VX ja AT vs Gemeinde Ummendorf*);

25.01.2024, C-687/21 (*MediaMarktSaturn*);

4.10.2024, C-200/23 (*Agentsia po vpisvaniyata vs OL*)

- Lühiajaline kontrolli kaotamine isikuandmete üle võib põhjustada andmesubjektile mittevaralist kahju.

20.04.2024, C-590/22 (*AT ja BT vs Ps GbR, VG, MB, DH, WB, GS*)

- Kartusest, et andmeid on avaldatud volitamata isikutele, ilma et avalikustamist oleks võimalik tõendada, piisab, et tekiks õigus hüvitisele, kui kartus koos selle negatiivsete tagajärgedega on piisavalt tõendatud.

8.01.2025, T-354/22 (*Bindl vs Komisjon)*

- Andmete edastamine kolmandasse riiki vastavaid nõudeid rikkudes asetas hageja „ebakindlasse olukorda“ seoses tema isikuandmete, eelkõige IP-aadressi töötlemisega.
- Mittevaralist kahju tuleb pidada tegelikuks ja kindlaks ning mittevaralise kahju suuruseks hinnata 400 eurot.

C-761/21 (*Juris GmbH*):

- Vastutava töötleja vastutusest vabanemiseks art 82(3) alusel ei piisa sellest, et kahju tuleneb rikkumisest, mille põhjustas vastutava töötleja töötaja (s.t. volituse all tegutsev isik art 29 tähenduses).

C-182/22 ja C-189/22 (*Scalable Capital*):

- Art 82 kohasel hüvitisel on eranditult kompensatsioonifunktsioon (tegemist pole karistusliku kahjuhüvitisega).
- Kui kahju on tuvastatav, kuid see ei ole suur, võib hüvitis olla väike, kui see kompenseerib kahju täielikult.

C-507/23 (*A vs Patērētāju tiesību aizsardzības centrs*)

- Vabandamine võib kujutada endast piisavat hüvitist mittevaralise kahju eest, eelkõige kui kahju tekkimisele eelnenud olukorda ei ole võimalik taastada ning tingimusel, et sellega kompenseeritakse täielikult tekkinud mittevaraline kahju.

# Riigikohtu halduskolleegiumi 26.09.2022 otsus asjas 3-20-1449 (X vs Sotsiaalkindlustusamet)

- 30.2. Kaebaja väidab, et **andmete õigusvastase edastamise tõttu tekkis tal ärevus ja stress iseseisva majandusliku toimetuleku pärast ning usaldamatus riigivõimu tegevuse vastu, kahjustada sai turvatunne (suhetes avaliku võimuga ja majandusliku toimetuleku aspektist) ning enda õiguste eest seismine on põhjustanud suurt pinget, tarbetut asjaajamist ja ebamugavusi**.
- 30.3. See, et kaebajal on puue (tundlikud eriliiki isikuandmed), oli kindlustusandjale kindlustuslepingu täitmisest tulenevalt varem teada. **Ainsaks kindlustusandjale varem mitte teada olnud faktiks oli teave puudetoetuse maksmise kohta - see asjaolu on kindlustusandjale teada olnud asjaolude ja õigusnormide koostoimest muul viisil üldjoontes järeldatav.** Kindlustusandja ei saanud seega lisateavet kaebaja tervisliku seisundi vms kohta.
- 30.4. **Usutav on, et õigusvaidlus tekitas kaebajas stressi, nördimust, ebakindlust jm sarnaseid üleelamisi. Sedalaadi ebameeldivused ei ole siiski iseenesest käsitatavad mittevaralise kahjuna**. Vastasel korral peaks mistahes õigusvaidlusega, mille inimene põhjendatult algatab, kaasnema suurem või väiksem rahaline hüvitis. Kehtiv õigus selleks alust ei anna. **Mittevaralise kahju hüvitamiseks peavad isikule põhjustatud tagajärjed olema tavapärasest eluriskist intensiivsemad**. Praegusel juhul ei ole kaebaja selliseid asjaolusid esile toonud.
- 30.5. **Eelkirjeldatud kaebaja hingelised üleelamised SKA õigusvastase tegevuse tagajärjel ei ületa lävendit, mida saab lugeda mittevaraliseks kahjuks VÕS § 128 lg 5 mõttes**.

# Riigikohtu halduskolleegiumi 21.06.2024 otsus asjas 3-22-2022

## (X kaebus Tartu Vangla vastu terviseandmete õigusliku aluseta töötlemisega tekitatud mittevaralise kahju hüvitamiseks)

- 27. /.../ Kaebaja on selgitanud, et **vangla tegevuse tulemusel tekkisid tal hingelised üleelamised ning usaldus psühholoogi vastu kadus, mistõttu ta ei julge enam psühholoogi juurde minna ega avameelne olla. Kaebajal on vaimse tervisega probleeme, mistõttu ta aga vajab psühholoogi abi. Kolleegium ei kahtle, et kaebajal tekkis kirjeldatud mittevaraline kahju. Kahju on põhjuslikus seoses vangla õigusvastase tegevusega**.
- 28. **Kuigi vastustaja õigusvastase tegevuse tulemusel tekkis kaebajal kahju, pole praegusel juhul siiski põhjust mõista mittevaralise kahju eest välja rahalist hüvitist. Piisab vastustaja tegevuse õigusvastasuse tuvastamisest** (HKMS § 41 lg 5).
- 28.1. /.../ Euroopa Liidu õiguses puuduvad õigusnormid, mille eesmärk on reguleerida kriteeriume makstava hüvitise ulatuse määramiseks. Seega on see liikmesriigi õiguse küsimus eeldusel, et järgitakse võrdväärsuse ja tõhususe põhimõtteid. (/.../) **Vastus küsimusele, kas rikkumine toob kaasa kahju hüvitamise rahas, oleneb Eesti õiguse järgi õigusrikkumise raskusest, süü vormist ja raskusest ning vastutust piiravatest asjaoludest** (/.../).
- 28.2. Ühest küljest on tegu terviseandmete kui eriliigiliste ja seega kõrgendatud kaitset vajavate isikuandmete õigusvastase töötlemisega (/.../). Arvestades rikkumise olemust, s.o patsiendisaladuse tuumaga võrreldava teabe säilitamine ja edastamine, **on kaebajal tekkinud üleelamised kindlasti olulised. Kahjustada sai ka kaebaja usaldus tulevikus psühholoogilise ravi saamisel** (/.../).
- 28.3. Teisalt seisneb vangla õigusvastane tegevus selles, et **vangla ei taganud, et kaebaja mõistaks õigesti vestluse ja seega andmetöötluse olemust**. /.../
- 28.4. Eeltoodust tulenevalt **tuleb vangla tegevus tunnistada osaliselt õigusvastaseks, s.o osas, milles vangla säilitas vangiregistris kaebaja vestlusest psühholoogiga lauseosad „tunnistas väga kergelt tekkivaid ärevushäireid“ ja „tunnistab, et konflikti korral tõstab häält“, võimaldas neile juurdepääsu vangiregistri põhimääruse alusel määratud vanglateenistujatele ning edastas neist esimese maakohtule**.

# Kollektiivsed esindushagid

- Tarbijate kollektiivsete huvide kaitsmise esindushagisid käsitlev direktiiv (EL) 2020/1828
- 01.01.2025 jõustusid tsiviilkohtumenetluse seadustiku (TsMS) muudatused
- Võimalik juhtudel, kui ettevõtjapoolne IKÜM-i rikkumine on kahjustanud või võib kahjustada andmesubjektide kollektiivseid huve.
- Kahte tüüpi kollektiivsed esindushagid:
  - Esindushagi rikkumise tuvastamiseks, lõpetamiseks, edasise rikkumise keelamiseks vms (s.t. ettekirjutusmeetmete saamiseks esitatud hagi) – ei sõltu kahju tekkimisest
  - Esindushagi individuaalsete õiguskaitsevahendite kindlaksmääramiseks (sh kahju hüvitamine)

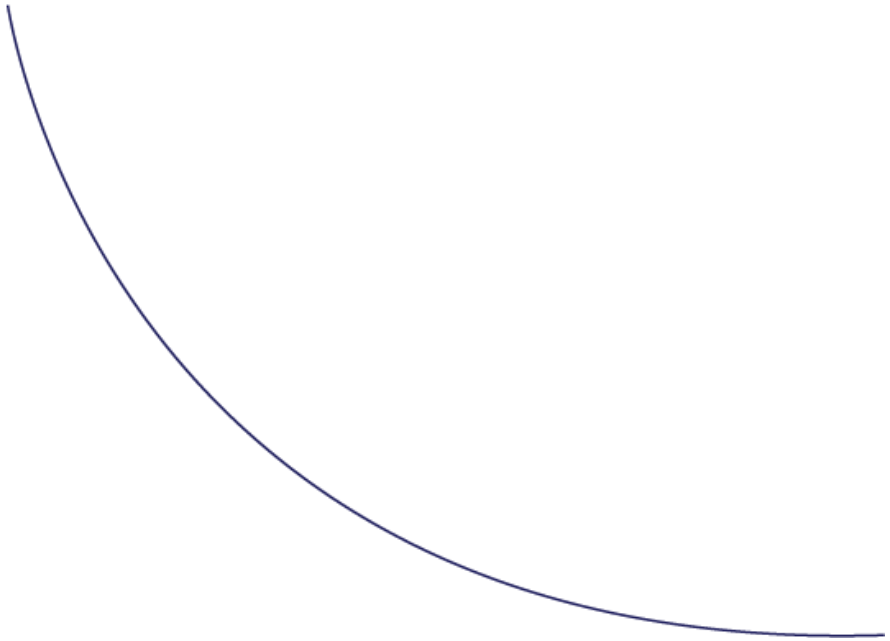
# Kollektiivsed esindushagid

- Riigisisese kollektiivse esindushagi andmesubjektide kollektiivsete huvide kaitseks võib esitada Andmekaitse Inspektsioon (IKS § $2^1$).
  - Laiemalt: vastavasse nimekirja kantud tarbijaühendused jt juriidilised isikud, TTJA, FI.
  - Piiriülesed pädevad üksused, kui nad on kantud Euroopa Komisjoni vastavasse nimekirja.
  - *Ad hoc* korras loodud sõltumatud pädevad üksused kohtu loal.
- **Hagita menetlus**: pädev üksus on **avaldaja** ning ettevõtja, kelle rikkumisest tulenevalt esindushagi esitati, on **puudutatud isik**.
  - Rikkumise tuvastamise ja lõpetamise esindushagide puhul ei kaasata menetlusse andmesubjekte.
  - Õiguskaitsevahendite kindlaksmääramise esindushagi menetlusega ühinenud andmesubjektidel on võimalik avaldusi ja taotlusi esitada (sh edasi kaevata ja täitemenetluses osaleda) üksnes pädeva üksuse vahendusel.
- Võimalik taotleda nii lõplikke kui ka ajutisi meetmeid (**esialgne õiguskaitse**).

# Kollektiivse esindushagi esitamise tingimused

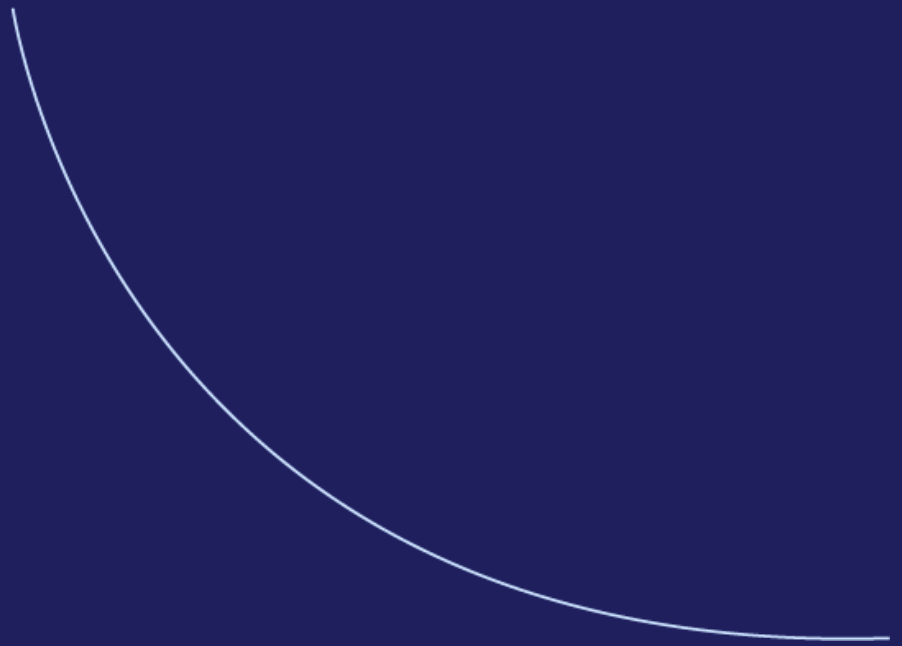
- Rikkumise tuvastamise ja lõpetamise või edasise rikkumise keelamise kollektiivse esindushagi menetluses ei pea avaldaja tõendama andmesubjektidele kahju tekkimist ega puudutatud isiku süüd.
- Individuaalsete õiguskaitsevahendite kindlaksmääramise esindushagi – kui asja arutamine kollektiivse esindushagina on **otstarbekas** ning **avaldusega liitub vähemalt 20 andmesubjekti**.
- Andmesubjektide nõuded peavad olema piisavalt sarnased ja seotud sarnaste fakti- või õigusküsimustega.

# Ühinemismudel



- Hilise *opt-in*-süsteemi mudel, kui esindushagiga taotletakse nii rikkumise tuvastamist kui ka õiguskaitsevahendite kindlaksmääramist
  - Esimeses menetlusetapis määratakse kindlaks rikkumine, tehakse siduv vaheotsus
  - Andmesubjekt saab menetlusega ka ühineda pärast esimest menetlusetappi
  - Määratakse tähtaeg andmesubjektide ühinemiseks õiguskaitsevahendite kindlaksmääramise menetlusega
  - Asja lõpetavas määruses määrab kohus kindlaks asjaga liitunud andmesubjektide individuaalsed õiguskaitsevahendid

# Kokkuvõte



- IKÜM art 82 on iseseisev kahjunõude alus. Nõude esitaja peab tõendama IKÜM-i rikkumise, tekkinud kahju ning põhjusliku seose.
- Tõendatud kartus isikuandmete võimalikust väärkasutusest võib olla mittevaraline kahju.
- Mittevaralise kahjuga ei pruugi alati kaasneda rahaline hüvitis.
- Praktika on alles kujunemisjärgus, Euroopas senised mittevaralise kahju hüvitised reeglina kuni paarsada eurot.
- Uus kollektiivsete esindushagide süsteem laiendab AKI pädevusi.
- Haldusmenetluse kõrvale tekib alternatiivne süsteem, mis võimaldab andmesubjektidel lihtsamini hüvitisi saada.

Aitäh!

Võta ühendust:

liisa.kuuskmaa@sorainen.com

SORAINEN 30

# Kohvipaus

SORAINEN

JUSTIITS- JA DIGIMINISTEERIUM

# Andmemäärusest

## EL määrus 2023/2854

Stina Avvo

IT-õiguse talituse juhataja

Tallinn, 01.04.2025

Tõhustada ELi andmepõhist majandust.

Edendada konkurentsivõimelist andmeturgu.

Muuta andmed kättesaadavamaks ja kasutatavamaks.

Soodustada andmepõhist innovatsiooni.

# Kellele mõeldud?

- **ühendatud toodete tootjad ja seotud teenuse osutajad**
  - turule lastud ELis
  - tootja ja teenuse osutaja asukohast olenemata
- **ühendatud toodete või seotud teenuste kasutajad**
  - ELis
- **andmevaldajad**
  - andmeid teevad kättesaadavaks ELis
  - andmevaldaja asukohast olenemata
- **andmesaajad**
  - ELis
- **avaliku sektori asutused, Euroopa Komisjon, Euroopa Keskpank ja liidu organid** ning **andmevaldajad, kes vastavad sellistele taotlustele**
  - erakorraline vajadus avalikes huvides oleva eriülesande täitmiseks
- **andmetöötlusteenuse osutajad**
  - olenemata nende asukohast
  - klient ELis
- **andmeruumides osalejad ja nutilepinguid kasutavad rakenduse müüjad, sh isikud, kelle kaubandus-, äri- või kutsetegevus** hõlmab kokkuleppe täitmise raames **nutilepingute kasutuselevõttu teiste jaoks**

# Määruse sisu

- Andmete jagamine ettevõtjate vahel ning ettevõtja ja tarbija vahel asjade interneti kontekstis
- Ettevõtete vaheline andmete jagamine
  - andmete jagamise tingimused, kui ettevõtja on seaduse, sealhulgas andmemääruse, alusel kohustatud jagama andmeid teise ettevõtjaga
- Ebaõiglaste lepingutingimuste sätted
- Ettevõtete ja valitsuse vaheline andmete jagamine
- Andmetöötlusteenuste vahetamine
  - pilv- ja servtöötlusteenuste osutajad peavad vastama miinimumnõuetele, et hõlbustada koostalitlusvõimet ja võimaldada teenuseosutaja vahetamist
- Kolmandate riikide valitsuste ebaseaduslik juurdepääs
  - ELis säilitatavad isikustamata andmed on kaitstud välisriikide valitsuste ebaseaduslike juurdepääsutaotluste eest
- Koostalitlusvõime sätted

# Liikmesriigid peavad...

- **nimetama ühe või mitu pädevat asutust**
  - sh vajadusel andmekoordinaator, kes tegutseb riiklikul tasandil ühtse kontaktpunktina
- **kehtestama karistusnormid**

# Ajakava

**12.09.2025**

- Üldine kohaldamine;
- Andmeid kättesaadavaks tegevate andmevaldajate kohustused (EList tulenevad kohustused või liidu õiguse alusel vastuvõetud riigisisesed õigusaktid, jõustuvad pärast 12.09.2025);
- Ebaõiglased lepingutingimused seoses andmetele juurdepääsu ja andmete kasutamisega ettevõtjate vahel - lepingute suhtes, mis on sõlmitud pärast 12.09.2025.

**12.09.2026**

- Kohustus teha toote kasutamisel loodud andmed ja seotud teenuse kasutamisel loodud andmed kasutajale juurdepääsetavaks - ühendatud toodete ja nendega seotud teenuste suhtes, mis lastakse turule pärast 12.09.2026.

**12.09.2027**

- Ebaõiglased lepingutingimused seoses andmetele ligipääsu ja andmete kasutamisega ettevõtjate vahel - lepingute suhtes, mis on sõlmitud 12.09.2025 või enne seda, eeldusel et lepingud:
  - a) on tähtajatud või
  - b) kaotavad kehtivuse vähemalt 10 a jooksul pärast 11.01.2024.

# Kasulikud materjalid

- Komisjoni vastused KKK-le
- Andmemääruse üldine tutvustus
- Andmemääruse tekst

JUSTIITS- JA DIGIMINISTEERIUM

# Tänan!

Stina Avvo

stina.avvo@justdigi.ee

# Tarneahela juhtimine andmekaitse ja küberturvalisuse vaatest – milleks kohustab GDPR ja uued küberturvalisuse õigusaktid?

Mihkel Miidla
Partner, vandeadvokaat

SORAINEN 30

## Miks on tarneahelaga seotud küberturvalisuse ja andmekaitsealaste riskide juhtimine järjest olulisem?

- Traditsiooniliselt on tarneahela puhul oluline – täitmise kvaliteet, kiirus, hind. Nüüd ka küberturvalisuse ja andmekaitse alased aspektid.
- Õigusaktid kohustavad nendes aspektides tarneahelaga tegelema. Kohati on ette nähtud ka kohustuslikud lepingutingimused.
- Suurenenud riskid, mis lähtuvad tarnijatest.
- Vastutus tarnija mittevastavuse eest.
  - Kõrged trahvimäärad.
  - Juhatuse vahetu vastutus (NIS2).
  - Vastutuse põhimõte (demonstreeri kooskõla!).
- Järelevalve aktiivsus kasvab.

| Õigusakt | Kohaldub | Mõju tarneahelale |
|---|---|---|
| **GDPR** | Vastutavad ja volitatud töötlejad | Andmetöötluslepingud, isikuandmete (piiriülene) edastamine, intsidentidest teavitamine |
| **NIS2** | Olulised ja elutähtsad üksused | Tarneahela turvalisus, intsidentidest teavitamine |
| **DORA** | Finantsasutused ja IKT teenusepakkujad | Kolmandate osapoolte IKT-riskide haldamine, sh kohustuslikud lepingutingimused |
| **Andmemäärus** | Andmevaldajad, kasutajad, andmesaajad, andmetöötlusteenuste osutajad | Kohustuslikud lepingutingimused |

*+AI määrus, CRA (küberkerksuse määrus), jt*

## Murekohad juristidele

- Tarnijate ja lepingute paljusus ning mitmekesisus
- Vanad, pikaajalised lepingud ei arvesta uute nõuetega (need peab avama)
- Alltöötlejate ja allhankijate jada (läbipaistmatu, palju isikuid jadas)
- Riskide (ja vastutuse) jaotus pole tasakaalus või on selgelt määratlemata
- Läbirääkimised aja- ja ressursimahukad
- Õigusaktide nõuete kattuvused ja vasturääkivused. Subjektiivsus ja sisustamata õigusmõisted.

# I. Uued lepingud

- Nõuetelevastavusega tuleks tegeleda juba hankimise faasis (RPF)
- Standardlepingud (vastavalt (tarnija) riskile)
  - Kohustuslikud lepingupunktid
- Tarnijate (eel-)hindamine (due diligence)
- KontrolInimekirjade kasutamine
- Järgida ka lähitulevikus kohalduma hakkavaid (uusi) nõudeid
- Kuidas käituda „tugevate“ tarnijatega, kes suruvad peale endale soodsaid tingimusi?

# II. Olemasolevad lepingud

- Esmane audit olemasolevatest lepingutest
  - Lünkade tuvastamine
- Prioritiseerimine – esmalt tegeleda kõrge riskiga tarnijatega/lepingutega.
- Tegevusplaan olemasolevate lepingute (ühepoolseks?) muutmiseks.
  - Standard lisa? *Ad hoc*?
- Valmistu vastuseisuks (*pushback*). Tihti soovivad tarnijad avada ka muud teemad.

# III. Pidev protsess

- Vastavuse jälgimise raamistik
  - Regulaarne tarnijate riskihindamine
  - Lepingu täitmise jälgimine (nt SLA, vastavusnäitajad)
  - Protsesside loomine intsidentide juhtimiseks
- Auditeerimine ja sertifikaadid
  - ISO 27001, SOC 2 või samaväärsete standardite kasutamine jälgimiseks
  - Lepingulised auditiõigused ja nende tõhus rakendamine
- Dokumentatsioon ja andmete säilitamine
  - Taga dokumentatsiooni olemasolu ja säilitamine
  - Sh hoolsuskohustuse täitmise kohta tõendite säilitamine
- Õigusalaste arengute jälgimine
  - Lepingute elutsükli haldus ja vajadusel lepingute muutmine/uuendamine lähtuvalt muutunud õiguslikest nõuetest.

## Soovitused

- Tarnijate kaardistamine ja esmane audit
- Kontrollnimekirjade kasutamine
- Standardlepingute ja -mallide kasutamine
- Juristide kaasamine ja vajalike ressursside tagamine! Juristide / õigusfunktsiooni järjest kasvav roll organisatsioonis (sh tootearendus). Koostöö teiste osakondade ja funktsioonidega on väga oluline
- Vastutuse põhimõttest tulenevalt - dokumenteerige kõik sammud/tegevused (ja tagage dokumentatsiooni säilitamine)!

Aitäh!

Võta ühendust:

mihkel.miidla@sorainen.com

SORAINEN 30

# Küberkindlustusest ja kindlustusjuhtumi haldamisest

Keio Kärdla
Howden Kindlustusmaakler OÜ, küberkindlustuse spetsialist

Oliver Ämarik
Soraineni kindlustusõiguse ekspert

# Küberkindlustus

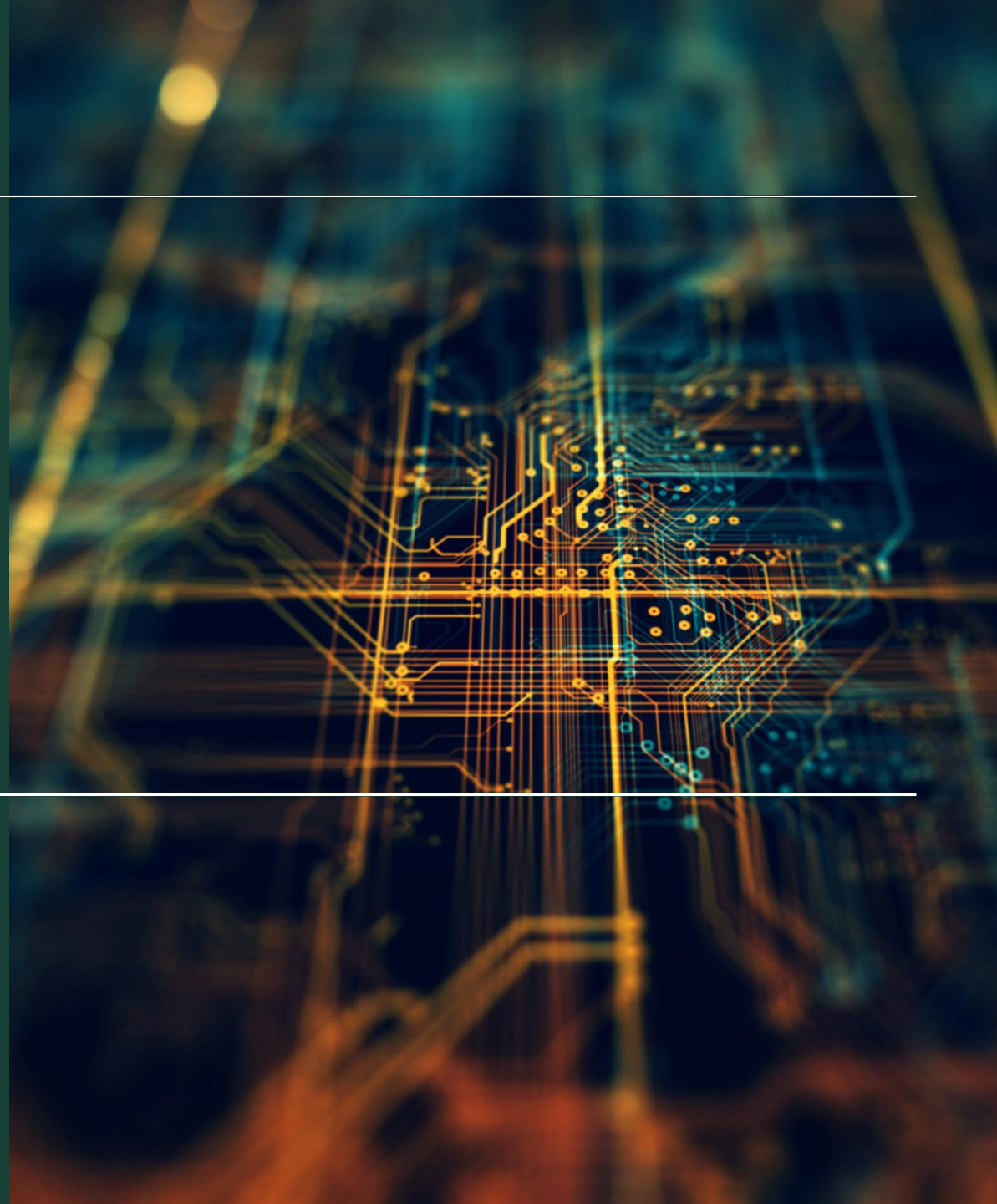
HOWDEN

# Keio Kärdla

Cyber Insurance Specialist (CCIS)

+372 5396 5880

keio.kardla@howdenestonia.ee



# Küberkindlustus

## Kriisi juhtimine

- 24/7 kriisiabi
- IT riskijuhtimine
- PR

## Esmase osapoole väljaminekud ja kulud

- Intsidentidele reageerimise kulud(kriminalistika, krediidiseire, PR, teavitus)
- Paranduse kulud
- Äritegevuse katkemine
- Suurenenud tööjõu kulud
- Viirused/Häkkimine
- Väljapressimine
- Seaduslikud uurimised ja trahvid

## Kolmanda osapoole vastutus

- Küber vastutus
- Privaatsuse vastutus
- Meedia vastutus
- Seaduslikud uurimised ja trahvid

# 4 küsimust

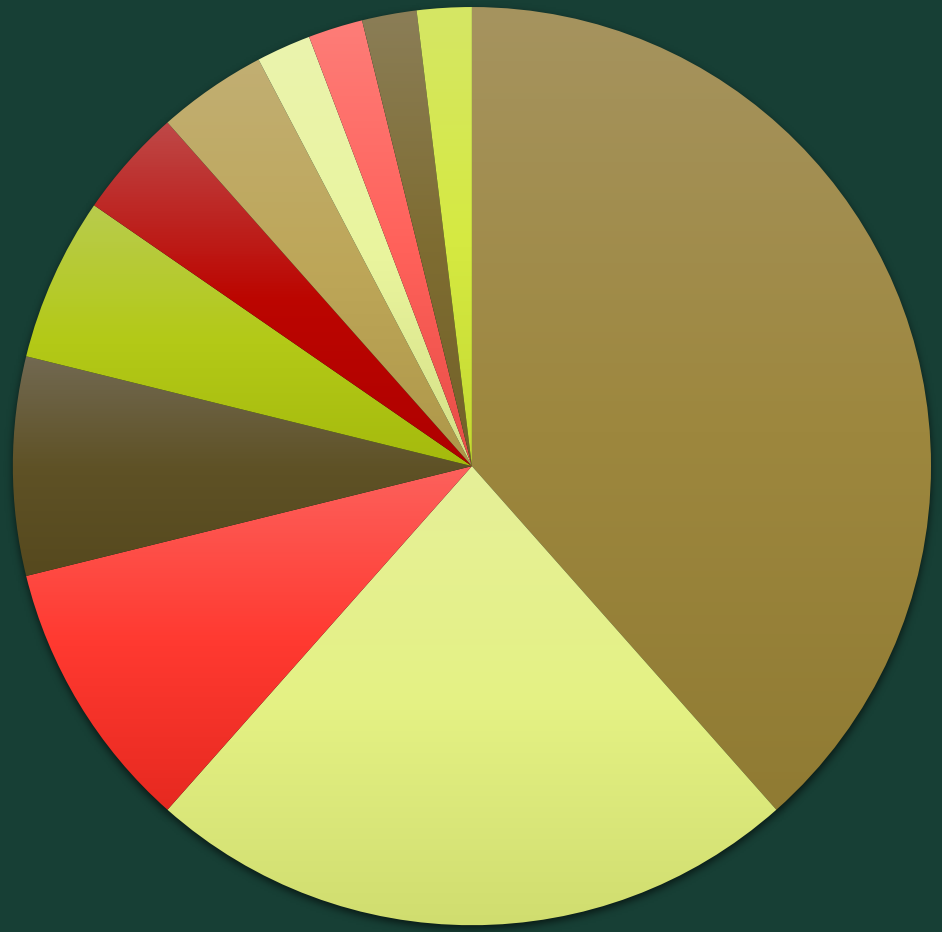
Ettevõtte nimi
Valdkond
Veebileht
Käive

## Esmased nõuded

- MFA (mitmikautentimine)
- EDR (otspunkti ohuavastus ja reageerimine; võrguturbe tehnoloogia lõppseadme pidevaks ohuseireks)
- IT/OT segmenteerimine (*tootmine)

*Nõuete osakaal suureneb vastavalt ettevõtte käibele

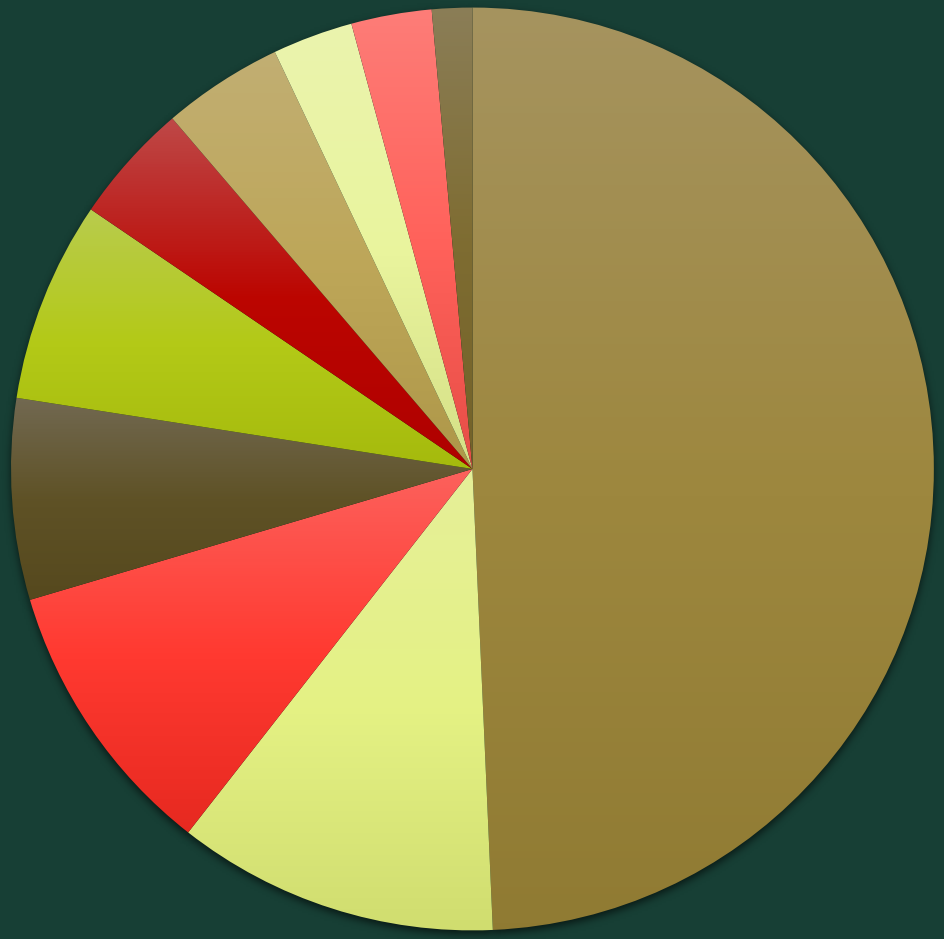
# Küberkindlustus



- Manufacturing & Distribution
- Business Services
- Healthcare
- Technology
- Telecommunications
- Retail
- Hospitality
- E-commerce
- Entertainment & Media
- Specialty Lines
- Manufacturing

**Beazley andmetele enim kahju kannatanud sektorid*

# Küberkindlustus




** Beazley andmetele peamised põhjused*

# Miks on küberkindlustus oluline?

Riskide maandamine

Küberteadlikus ja hügieen

Valmidus kõige hullemaks

Süsteemide arendamine

Ajaga kaasas liikumine

# Välistused

Sõjaklausel

*sõda, sissetung, välisvaenlase tegevus, vaenutegevus (olenemata sellest, kas sõda on välja kuulutatud), kodusõda, mäss, revolutsioon, vastuhakk, sõjalise või anastatud võimu kasutamine, vara konfiskeerimine, natsionaliseerimine, rekvireerimine, hävitamine või kahjustamine mis tahes valitsus- või avaliku või kohaliku asutuse korraldusel; tingimusel et seda välistust ei kohaldata küberterrorismi suhtes;*

*selle välistuse kohaldamisel tähendab küberterrorism häiriva tegevuse ettekavatsetud kasutamist või häiriva tegevuse kasutamise ohtu mis tahes arvutisüsteemi või võrgu vastu, et tekitada kahju, saavutada sotsiaalseid, ideoloogilisi, usulisi, poliitilisi vms eesmärke või heidutada mõnd füüsilist või juriidilist isikut selliste eesmärkide poole pürgimisel;*

“

# Tehes mitte midagi, selle hind on liiga kõrge

# Küberkindlustus: kindlustusjuhtum ja selle haldamine

Oliver Ämarik
Advokaat

SORAINEN 30

# #1. Intsidendi tuvastamine

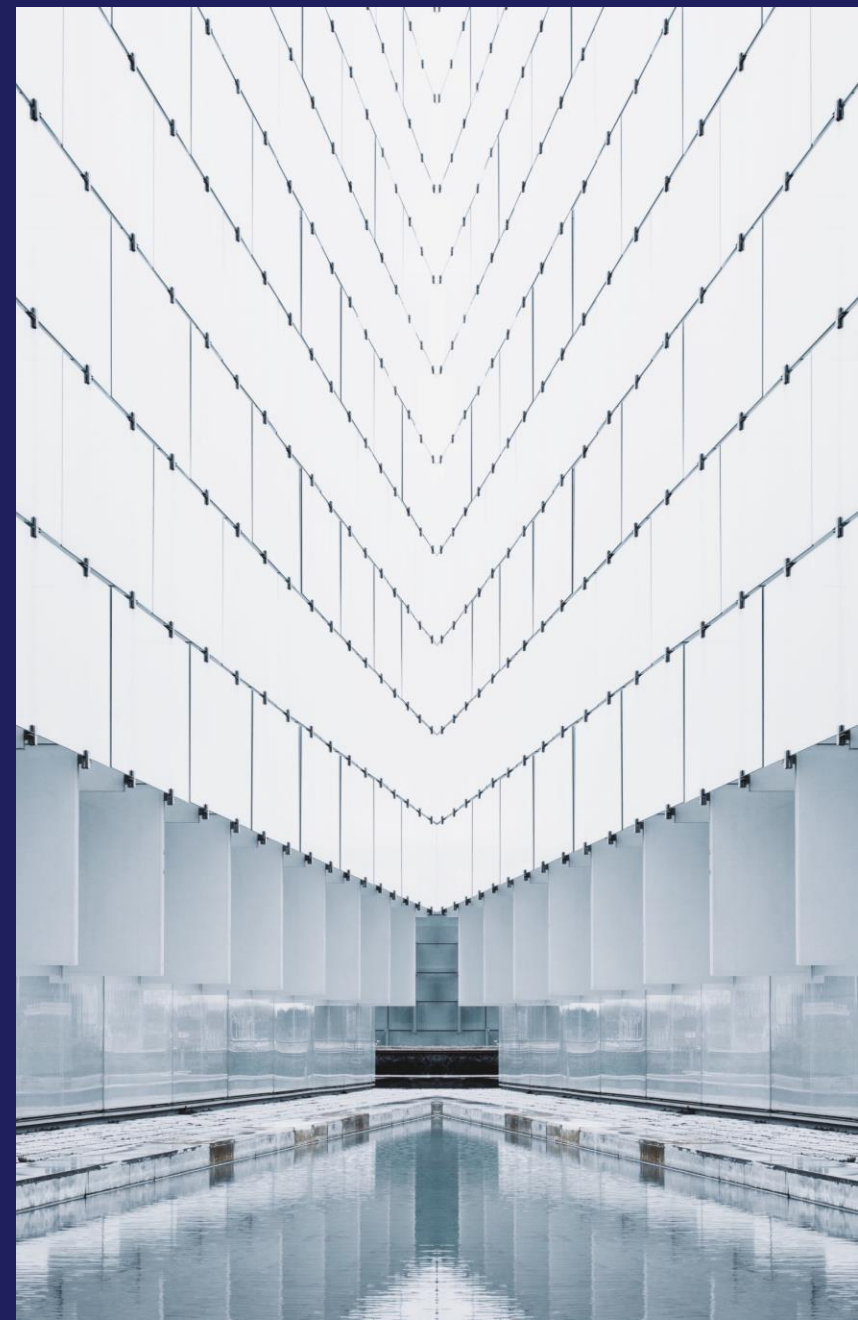
Kindlustusvõtja peab kõigepealt hindama, kas tegemist on võimaliku kindlustusjuhtumiga. Levinud küberintsidentide hulka kuuluvad:

(i) andmekaitserikkumised (volitamata juurdepääs tundlikele andmetele);

(ii) lunavararünnakud;

(iii) andmepüügi tagajärjel pettuslike tehingute tegemine;

(iv) teenustõkestusründed (DDoS).



# #2. Kindlustusandja teavitamine

Kindlustusandja **viivitamatu** teavitamine kasutades selleks kindlustuslepingus määratud küberintsidendi teavitamise kanalit.

**Esialgse teabe edastamine:**

i. intsidendi olemus (näiteks lunavara, andmeleke).

ii. aja- ja tegevuskava (millal avastati, kuidas arenes).

iii. mõjutatud süsteemid ja andmed (kahju ulatus).

iv. tegevused siiani (kahju piiramise meetmed, kas on kaasatud kolmandaid osapooli).

Kui teavitamine hilineb, võib see **ohustada kindlustuskaitset**.

# #3. Juhtumi haldamine

Küberkindlustuse lepingud sisaldavad sageli **eelnevalt heaks kiidetud teenusepakkujaid**, kelle juurde kindlustusandja kindlustusvõtja suunab juhtumi haldamiseks:

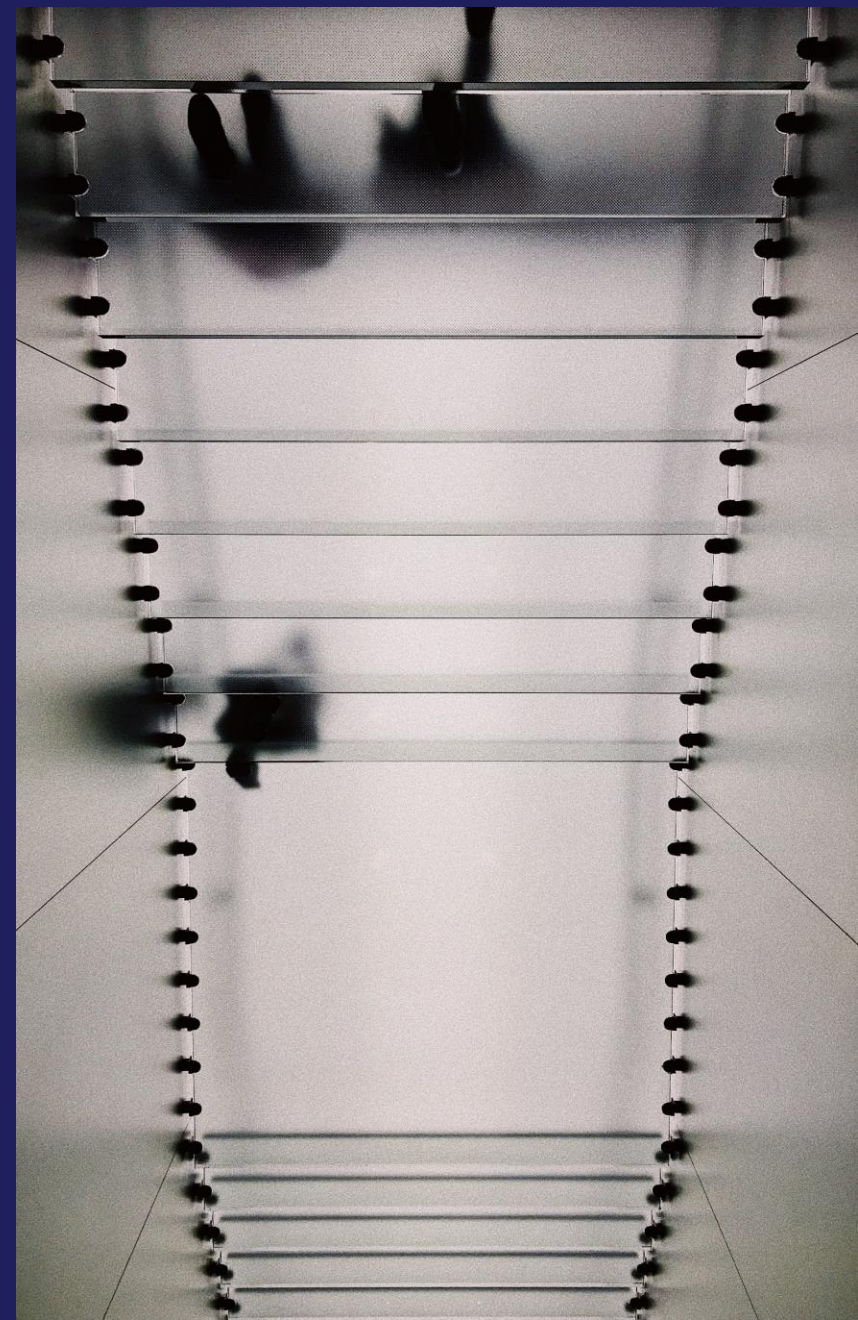
i. Intsidendi haldamine (juhtumi lahendamine);

ii. IT-ekspertiis (ründe meetodite ja ulatuse selgitamiseks, ründe piiramiseks, lõpetamiseks);

iii. Õigusnõustajad (vastutuse ja regulatiivsete kohustuste osas);

iv. Suhtekorraldajad (mainekahju maandamiseks; kriisikommunikatsioon).

NB! Teiste teenuseosutajate kasutamisel kooskõlastus.



# #4. Nõude esitamine ja dokumenteerimine

- Kindlustusvõtja peab esitama selgeid tõendeid (näiteks IT-ekspertide raportid, suhtlus järelvalvega), et toetada oma nõuet.
- Kui äritegevus oli häiritud, on vaja dokumenteerida saamata jäänud tulu (arvutused) ja meetmed, mida rakendati olukorra leevendamiseks.
- Sündmuse tagajärjel kantud kulud (nõustamisteenused, trahvid jm)

# #5. Regulatiivsete ja juriidiliste kohustuste täitmine

**Andmelekketeavitused**

Kui isikuandmed on kompromiteeritud, võib olla kohustus teavitada:

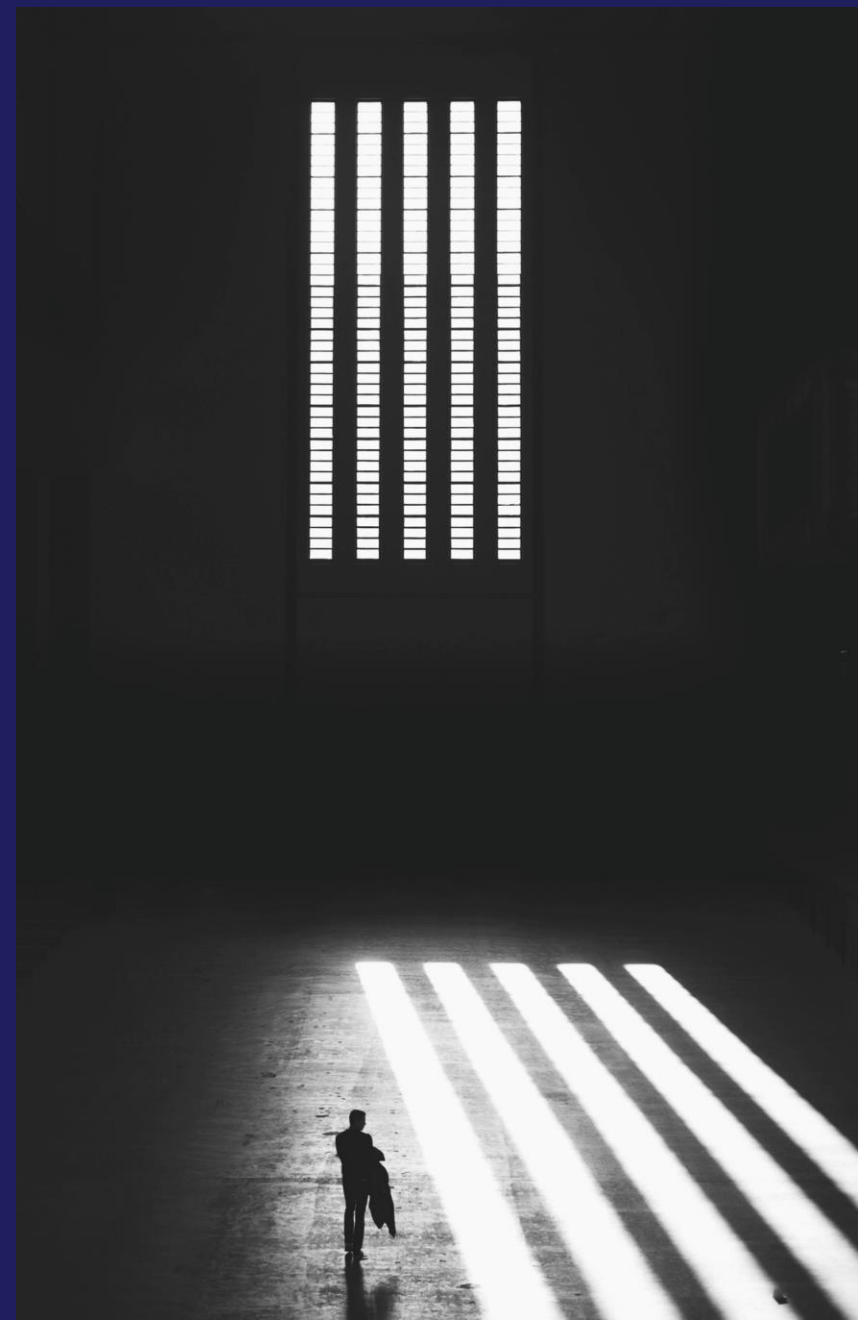
- Andmekaitse järelevalveasutusi (nt GDPR nõuab teavitamist 72 tunni jooksul; NIS2 puhul isegi kiiremini);
- Mõjutatud kliente või partnereid.

**Õiguskaitseasutuste kaasamine**

Kui tegemist on kuritegeliku tegevusega (näiteks lunavara, pettus), võib soovitatav olla teavitada õiguskaitseorganeid (küberkuritegevuse üksused, politsei).

**Kolmandate osapoolte nõuete haldamine**

Kui rünnak mõjutab kliente, tarnijaid või partnereid, võib selle tagajärjel tekkida erinevaid täiendavaid kolmanda isiku nõudeid. Kindlustusvõtja tsiviilõiguslik vastutus, vaidlused.



# #6. Hüvitamine

**Hüvitise väljamakse**

Kindlustusandja hindab tõendeid ja otsustab, kas kahju kuulub poliisi alusel hüvitamisele. Vaidlused võivad eelkõige tekkida, kui kindlustusandja leiab, et ettevaatusabinõusid ei järgitud või kindlustusvõtja on esitanud ebaõiget teavet.

**Hüvitised**

Kui nõue on heaks kiidetud, võib poliis katta:

i. intsidentide halduskulud (ekspertiisid, juriidiline tugi, PR);

ii. lunaraha;

iii. ärikatkestuse kahjud;

iv. regulatiivsed trahvid.

# #7. Kokkuvõte

**Peamised meeldetuletused kindlustusvõtjale:**

i. Tegutse kiiresti – kindlustusandjat tuleb teavitada kohe.

ii. Kasuta kindlustusandja poolt heakskiidetud teenusepakkujaid.

iii. Dokumenteeri kõik – tõendid aitavad intsidendi haldamisel ja nõude esitamisel ning selle rahuldamisel.

iv. Mõista poliisi tingimusi ja välistusi.

v. Õpi juhtumist ja tugevda turvameetmeid.

Aitäh!

Võta ühendust:
oliver.amarik@sorainen.com

SORAINEN 30

Osale ka meie järgmisel ärihommikul!

Lisainfo:
https://www.sorainen.com/et/uritused/

Vaata ärihommikute ja veebiseminaride salvestusi järele:

Spotify.com

YouTube.com

SORAINEN

Sorainen.com

Mihkel Miidla
mihkel.miidla@sorainen.com

Oliver Kuusk
oliver.kuusk@sorainen.com

Liisa Maria Kuuskmaa
liisa.kuuskmaa@sorainen.com

Oliver Ämarik
oliver.amarik@sorainen.com


SORAINEN 30

SORAINEN 30