Millised muudatused toob kaasa isikuandmete kaitse üldmäärus kiirabi töös?

Konverents Kiirabi 2018

Ingeri Luik-Tamme, vandeadvokaat, advokaadibüroo TGS Baltic

Isikuandmete kaitse regulatsioon – minevik ja olevik

Minevik:

- Andmekaitsedirektiiv 95/46/EÜ
- Isikuandmete kaitse seadus (IKS)
- Erinormid erinevates seadustes

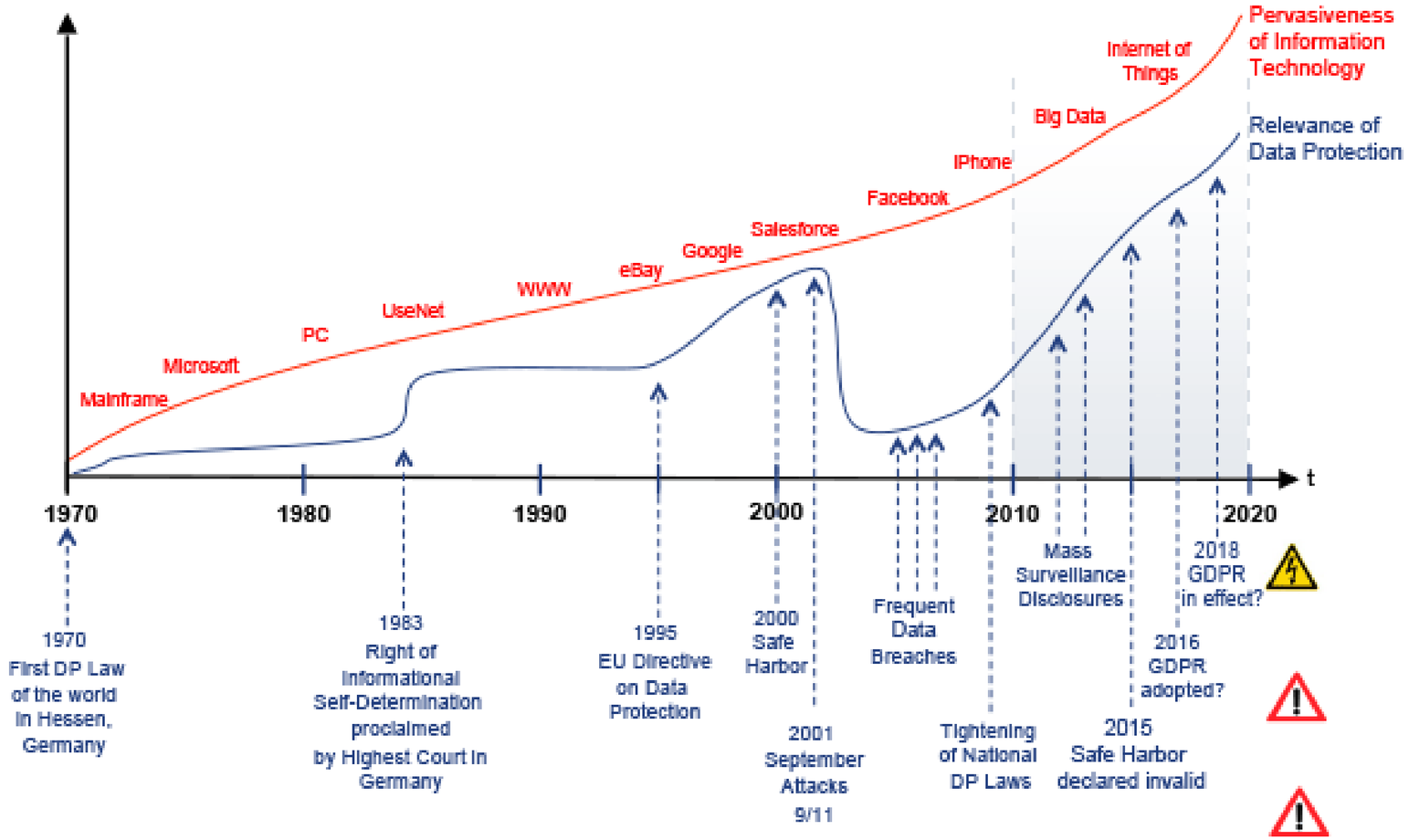
Olevik:

- Isikuandmete kaitse üldmäärus (ingl. k. General Data Protection Regulation – GDPR) - otsekohalduv kogu Euroopa Liidus alates 25. mai 2018
- Üldmääruse rakendamise seadus – uus isikuandmete kaitse seadus (hetkel veel eelnõu staadiumis)
- Erinormid erinevates seadustes

TGS BALTIC
VARUL GRUNTE SUTKIENE

Milleks uus regulatsioon?

GDPR – ajalooline taust



Andmelekked tervishoiusektoris

- **Ameerika Ühendriigid**
  - 2015 Anthem: varastati 78,8 miljoni patsiendi ravidokumendid
  - 2015 University of California, Los Angeles Health: varastati 4,5 miljoni patsiendi andmed

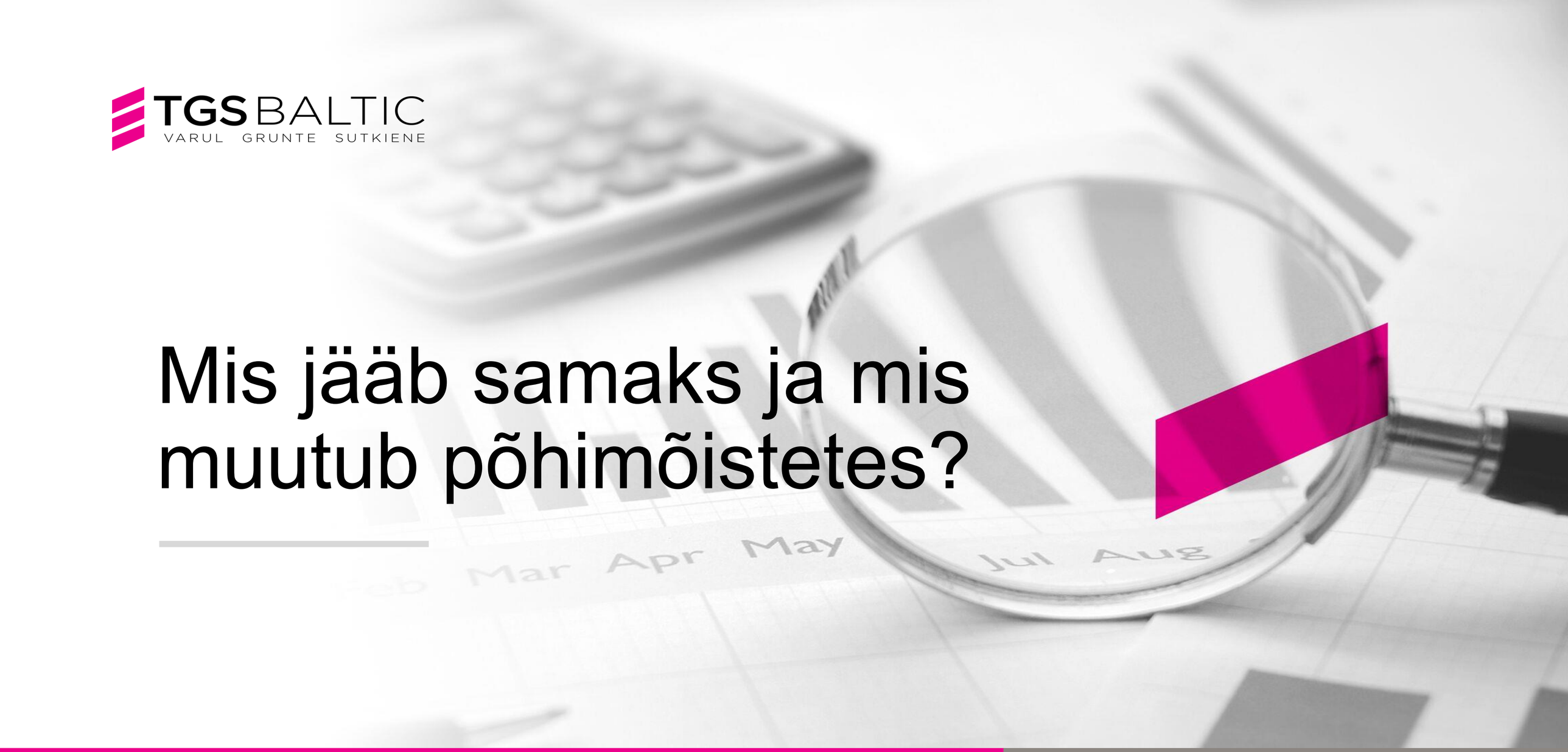
- **Euroopa**
  - 2018 Helse Sør-Øst RHF (Norra): 3 miljoni patsiendi võimalik andmete leke
  - 2017 Grožio Chirurgia (Leedu): varastati ilukirurgia kliiniku 25 000 patsientide andmed

Isikuandmete kaitse – mida või keda me kaitseme?

- Eesmärk on kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusele.
- Isikuandmete kaitse eesmärgiks ei ole kaitsta andmeid, vaid kaitsta inimest, keda kaitstavad andmed identifitseerivad ja mille kaudu isik ennast teistele isikutele määratleb.
- GDPR-i läbivateks eesmärkideks on ettevõtete vastutustundlikkuse suurendamine ja inimesele oma andmete üle suurema kontrolli andmine.

TGS BALTIC
VARUL GRUNTE SUTKIENE

Mis jääb samaks ja mis muutub põhimõistetes?



Mis on isikuandmed?

- Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta
- Tuvastatavuse kriteerium: tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal
- Teave füüsilise isiku kohta on isikuandmed sõltumata teabe vormist (kirjalikud andmed, foto, video) ja asukohast (dokumendis, e-kirjas, andmekandjal)

Isikuandmete liigitus

- **Eriliigilised isikuandmed** (varasemalt: delikaatsed isikuandmed)
  - Eriliigiliste isikuandmete kontseptsioon põhineb vajadusel anda teatud laadi andmetele suurem kaitse.
  - Eriliigilised isikuandmed: rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, **geneetilised andmed**, **biomeetrilised andmed**, **terviseandmed**, **andmed füüsilise isiku seksuaalelu ja seksuaalse orientatsiooni kohta**

- **Tavalised isikuandmed**
  - mis tahes muud andmed inimese kohta, mis ei ole eriliigilised isikuandmed (nt nimi, sünniaeg, isikukood, näofoto, aadress, perekonnaseis, majanduslik seisund)

Isikuandmete töötlemine

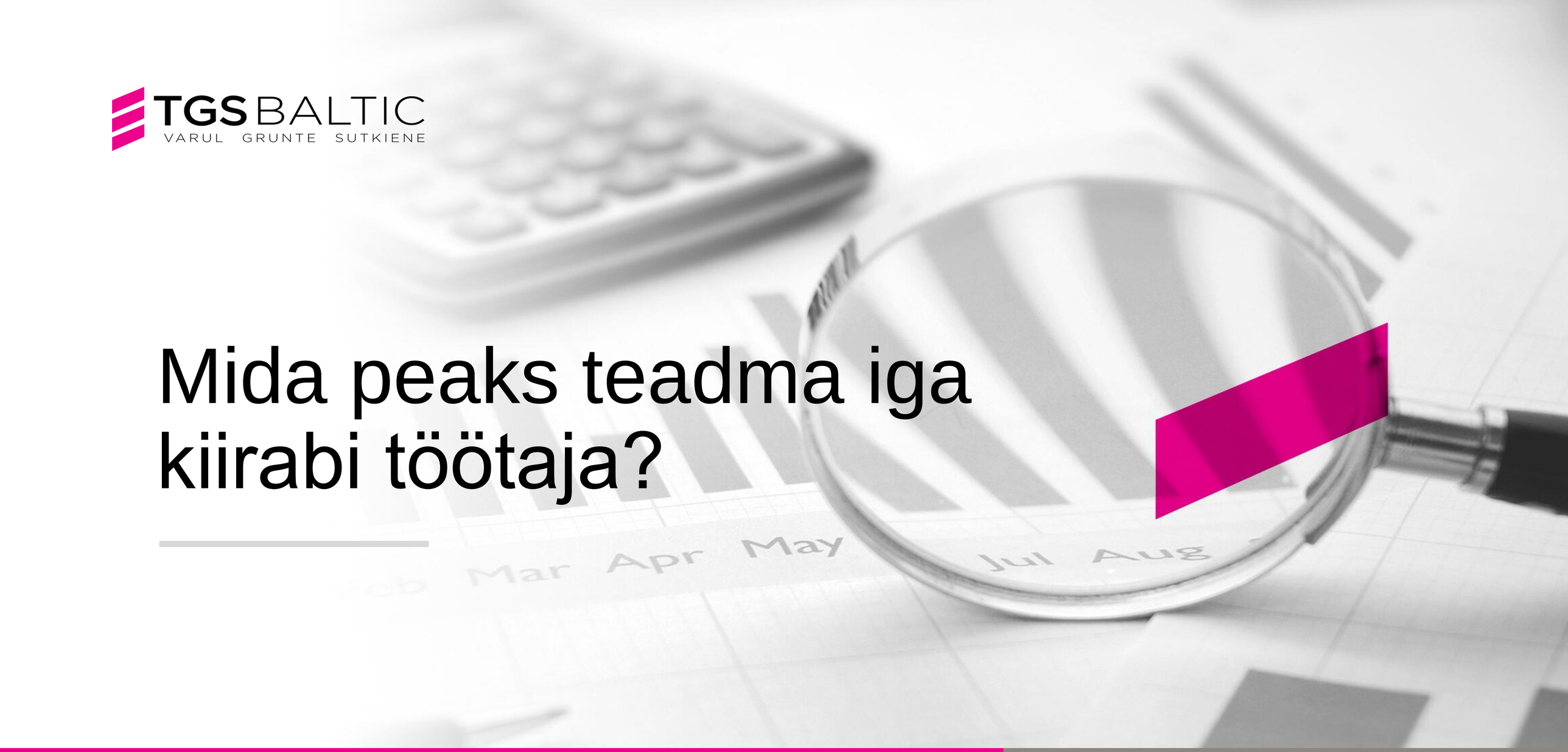
- **Isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas:**
  - Kogumine
  - Dokumenteerimine
  - Korrastamine
  - Struktureerimine
  - Säilitamine
  - Kohandamine
  - Muutmine
  - Päringute tegemine
  - Lugemine
  - Kasutamine
  - Edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine
  - Ühitamine või ühendamine
  - Piiramine
  - Kustutamine
  - Hävitamine

Isikuandmete töötleja

- **Vastutav töötleja** (*controller*):
  - füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid; kui sellise töötlemise eesmärgid ja vahendid on kindlaks määratud liidu või liikmesriigi õigusega, võib vastutava töötleja või tema määramise konkreetsed kriteeriumid sätestada liidu või liikmesriigi õiguses
- **Kaasvastutavad töötlejad** (*joint controllers*)
  - määravad andmetöötluse eesmärgid ja vahendid ühiselt. Jaotatakse omavahel kohustuste ulatus. Andmesubjekti ees vastutavad ühiselt (solidaarvastutus)
- **Volitatud töötleja** (*processor*):
  - füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.

TGS BALTIC
VARUL GRUNTE SUTKIENE

Mida peaks teadma iga kiirabi töötaja?



Isikuandmete töötlemise põhimõtted

- Seaduslikkus, õiglus ja läbipaistvus (*lawfulness, fairness, transparency*)
- Eesmärgi piirang (*purpose limitation*)
- Võimalikult väheste andmete kogumine (*data minimisation*)
- Õigsus (*accuracy*)
- Säilitamise piirang (*storage limitation*)
- Usaldusväärsus ja konfidentsiaalsus (*integrity and confidentiality*)

Isikuandmete töötlemise õiguslikud alused

- Andmesubjekti nõusolek
- Vajalik andmesubjektiga sõlmitud lepingu täitmiseks
- Vajalik vastutava töötleja juriidilise kohustuse täitmiseks (st õigus tuleneb seadusest)
- Vajalik andmesubjekti või muu füüsilise isiku eluliste huvide kaitsmiseks
- Vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks
- Vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral

Isikuandmete töötlemine seaduse alusel

- **Tervishoiuteenuste korraldamise seadus § 41. Isikuandmete töötlemine**

  (1) Tervishoiuteenuse osutajal, kellel on seadusest tulenev saladuse hoidmise kohustus, on õigus **andmesubjekti nõusolekuta** töödelda tervishoiuteenuse osutamiseks vajalikke isikuandmeid, sealhulgas delikaatseid isikuandmeid.

- **Tervise infosüsteemi põhimäärus § 11. Tervishoiuteenuse osutaja õigus andmetele juurdepääsuks**

  Tervishoiuteenuse osutajal on tervise infosüsteemis olevatele isikuandmetele juurdepääs tervishoiuteenuse osutamise lepingu sõlmimiseks ja täitmiseks.

Patsientide andmete kasutamine

- Tervishoiuteenuse osutaja andmebaas ja TIS
- Tervishoiuteenuse osutaja andmebaasi kasutamist saab reguleerida tervishoiuteenuse osutaja ise
- TIS-i kasutamist reguleerib tervise infosüsteemi põhimäärus (st õigusakt)

Patsiendi õigused TIS-i dokumentide osas

- Patsiendil on juurdepääs oma isikuandmetele tervise infosüsteemis
- Patsiendil on õigus keelata tervishoiuteenuse osutaja juurdepääs TIS-is olevatele isikuandmetele
- Kui patsient väljendab sellist tahet, siis on tervishoiuteenuse osutajal kohustus kohe keelata juurdepääs tema koostatud ning tervishoiuteenuse osutamise lepingu raames koostatud ja edastatud dokumentidele
- **Tahteavaldus peab olema kirjalik**

Tervishoiuteenuse osutaja ja arsti juurdepääs TIS-i dokumentidele

- Tervishoiuteenuse osutajal on juurdepääs tervise infosüsteemis olevatele isikuandmetele tervishoiuteenuse osutamise lepingu sõlmimiseks ja täitmiseks
- Tervishoiuteenuse osutaja peab tagama, et nimetatud juurdepääsuõigust teostatakse üksnes tervishoiuteenuse osutamise lepingu sõlmimiseks ja täitmiseks
- Oluline säilitada andmed tervishoiuteenuse osutamise lepingu sõlmimise kohta

Tervishoiuteenuse osutaja ja arsti juurdepääs TIS-i dokumentidele

- Tervishoiuteenuse osutajal on õigus salvestada andmeid tervise infosüsteemist, kui see on vajalik tervishoiuteenuse osutamise lepingu sõlmimiseks või täitmiseks
- Muul eesmärgil (nt eriarsti arvamuse saamine) juurdepääs lubatud ei ole
- AKI aastaraamat 2016: Kokku lõpetasime 2016. aastal 7 digiloo väärkasutamisega seotud väärteomenetlust. Kõigi nende menetluste raames said tervishoiutöötajad karistatud rahatrahviga

Patsiendi kui andmesubjekti õigused

- Õigus saada teavet ja tutvuda andmetega
- Õigus andmete parandamisele
- Õigus andmete kustutamisele („õigus olla unustatud“)
- Õigus isikuandmete töötlemise piiramisele
- Andmete ülekandmise õigus
- Õigus esitada vastuväiteid
- Õigus, et isiku kohta ei võetaks vastu otsust, mis põhineb üksnes automatiseeritud töötlusel, sh profiilianalüüsil

Teavitamiskohustus ja privaatsuspoliitika

- GDPR-i alusel on igal isikuandmete töötlejal kohustus teavitada inimest (patsienti) tema isikuandmete töötlemise detailidest
- Kui andmeid kogutakse andmesubjektilt endalt, tuleb teavitamine läbi viia andmete saamise ajal
- Tervishoiuteenuse osutajal on mõistlik teavitamiskohustuse täitmiseks välja töötada avalik privaatsuspoliitika dokument või lülitada privaatsuspoliitika teenuse osutamise üldtingimustesse
- Kui andmete töötlemise aluseks on nõusolek, tuleks teave esitada ka nõusoleku juures

Privaatsuspoliitika

- Annab ülevaate:
  - Millistest allikatest on isikuandmed saadud
  - Kes on andmete töötlejaks ja kuidas temaga ühendust võtta
  - Millisel eesmärgil ja õiguslikul alusel inimese andmeid töödeldakse
  - Kui kaua andmeid säilitatakse
  - Kellele, millistel juhtudel ja viisidel andmeid edastatakse
  - Missugused on andmesubjekti õigused tema andmete töötlemise suhtes
  - Kas isikuandmete esitamine inimese poolt on kohustuslik ja millised on andmete mitte-esitamise tagajärjed
  - Automatiseeritud otsuste tegemise loogikast (asjakohasel juhul)

Eesti Arstide Liit. Eesti arstieetika koodeks p. 2:

- „Arst peab selgitama patsiendile tema tervislikku seisundit ning saama vabatahtlikult antud ja arusaamisel põhineva nõusoleku vajalike uuringute ja ravimenetluste tegemiseks. Patsiendile antav informatsioon peab hõlmama teavet tema kohta käivate **andmete kogumisest, säilitamisest ja kasutamisest** (sealhulgas tervise infosüsteemis) ning uuringute ja ravi vajalikkuse, võimalike erinevate raviviiside, samuti nende võimalike kõrvalnähtude, tüsistuste ja ohtude kohta. Kui patsient tasub ravi eest ise, tuleb teda enne selle hinnast teavitada.“

Patsiendi õigused seoses andmetega

- Teovõimelisel patsiendil on õigus:
  - dokumentidega tutvuda ja;
  - saada neist oma kulul ärakirju, kui seadusest ei tulene teisiti

- Erand – psühhiaatrilise abi seadus § 4 p 2:
  - psühhiaatrilist abi saaval isikul on õigus tutvuda temasse puutuvate ravidokumentidega, välja arvatud juhul, kui see võib osutuda kahjulikuks tema vaimsele tervisele või teiste isikute julgeolekule.

Lähedaste ja kolmandate isikute õigused seoses andmetega

Haiglas viibiv patsient:

- Edastamine või juurdepääs on lubatud lähedastele, va kui:
  - patsient on edastamise või juurdepääsu keelanud
  - uurimisorgan on edastamise või juurdepääsu keelanud

Muudel juhtudel:

- Edastamine või juurdepääs on lubatud:
  - Alaealise seaduslikele esindajatele (kui ise ei ole piisavalt vastutusvõimeline)
  - Piiratud teovõimega isiku seaduslikule esindajale (kui eestkoste hõlmab seda valdkonda)
  - Kui esineb muu seaduses sätestatud alus

Töötlustoimingute register

GDPR

- **AKI-s registreerimise kohustus lõpeb/puudub**
- Kohustus luua ettevõttesisene elektrooniline töötlustoimingute register
- Kohustus registreerida registris kõik isikuandmete töötlustoimingud (sõltumata andmete liigist)

IKS

- Kohustus registreerida delikaatsete isikuandmete töötlemine või vastutava isiku määramine AKI-s
- Kohustus esitada andmed töötlemise ja kasutatavate turvameetmete kohta

Andmete töötlemise kaardistamine

- Millised ettevõtte tegevused on seotud isikuandmetega
- Millistest allikatest ettevõte andmeid saab (inimeselt endalt, lepingupartneritelt, avalikest registritest või muudest avalikest allikatest)
- Millisel alusel ja eesmärgil andmete töötlemine toimub
- Millises rollis on ettevõte andmete töötlemisel – vastutava või volitatud töötleja rollis
- Kellele ja millisel viisil andmeid edastatakse
- Millistes seadmetes ja tarkvaras andmeid töödeldakse

Ettevõtte sisesed reeglid isikuandmete töötlemiseks

- Tuleks tagada, et:
  - Olemas oleksid üldised andmekaitsega seonduvad reeglid (sh käitumisjuhend andmekaitse alase nõude esitamise ja rikkumise korral)
  - Iga töötaja tegevust reguleerivates dokumentides oleksid kirjas andmete töötlemisega seotud õigused (milliste andmetega on õigus tutvuda ja toiminguid teha)
  - Iga töötaja teaks oma andmekaitsega seonduvaid kohustusi (konfidentsiaalsuskohustus, andmesubjektidele teabe andmise kohustus, registri täiendamise vajadusest teavitamine, mõjuhinnangu läbiviimise hindamine, rikkumistest teavitamine jne)
  - Töötajad oleksid kursis töötlustoimingute registriga ja kohustusega seda täiendada, kui alustatakse uue andmetöötlusprotsessiga

Andmekaitseametnik (andmekaitsespetsialist)

- Andmekaitseametnik (andmekaitsespetsialist) tuleb määrata kui:
  - isikuandmeid töötleb avaliku sektori asutus või organ (v.a kohus)
  - ettevõtte põhitegevuseks on ulatuslik andmesubjektide korrapärane ja süstemaatiline jälgimine
  - ettevõtte põhitegevuseks on andmete eriliikide ulatuslik töötlemine
- Andmekaitseametnik võib olla andmetöötleja koosseisuline töötaja või täita ülesandeid teenuslepingu alusel
- Andmekaitseametnik on andmekaitsealaseid õigusakte ja tavasid eksperdi tasandil tundev isik, kes abistab ja kontrollib andmetöötlejat määruse täitmisel
- Andmekaitseametnikul peab olema võimalik täita oma kohustusi ja ülesandmeid sõltumatul viisil

Rikkumiste dokumenteerimine ja teavitamiskohustused

- Absoluutselt kõik rikkumised (andmete leke, andmete kaotsiminek või kustumine vms) tuleb ettevõtte siseselt **dokumenteerida** (nt töötlustoimingute registris)
- Juhul, kui rikkumine kujutab endast tõenäoliselt ohtu inimese õigustele ja vabadustele, tuleb 72 tunni jooksul **teavitada rikkumisest Andmekaitse Inspektsiooni.**
- Juhul, kui rikkumine kujutab endast tõenäoliselt suurt ohtu inimese õigustele ja vabadustele, tuleb üldjuhul viivitamatult **teavitada rikkumisest ka andmesubjekti.**

Käitumisjuhised rikkumiste korral

- 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
- Koheselt tuleb teha kindlaks rikkumise asjaolud ja võtta tarvitusele meetmed rikkumise kõrvaldamiseks, edasiste rikkumiste vältimiseks ning kahju minimeerimiseks

Rikkumiste dokumenteerimine ja rikkumise teade

- Teates tuleb esitada järgmine teave:
  - Rikkumise laad
  - Puudutatud andmesubjektide kategooriad ja ligikaudne arv
  - Puudutatud isikuandmete kirjete liigid ja ligikaudne arv
  - Isikuandmetega seotud rikkumise võimalikud tagajärjed
  - Tarvitusele võetud või plaanitavad meetmed rikkumise kõrvaldamiseks ja rikkumise kahjuliku mõju leevendamiseks
  - Andmekaitseametniku või muu kontaktisiku, kelle käest saab täiendavat teavet, nimi ja kontaktandmed
- Rikkumise ettevõtte sisesel dokumenteerimisel, isegi kui ei ole teavitamiskohustust, on soovitatav dokumenteerida samad andmed.

Järelevalve isikuandmete töötlemise nõuete täitmise üle

- Andmekaitse Inspektsioon (AKI)
- Isikuandmete töötlemise nõuete rikkumise korral on järelevalveasutusel õigus kasutada mitmeid sunnimeetmeid, sh:
  - hoiatus
  - noomitus
  - korraldus puuduste kõrvaldamiseks
  - töötlemise piirangute kehtestamine
- Lisaks nimetatud sunnimeetmetele või nende asemele on õigus määrata rahalisi sanktsioone – trahve

Trahvid

- Võrreldes kehtivate trahvimääradega on summad oluliselt kõrgemad
- Trahvi saab määrata nii tahtliku rikkumise kui hooletuse puhul
- Rikkumise kategooriad ja trahvimäärad:
  1) Nö kergemad rikkumised – kuni 10 miljonit eurot või kuni 2% ettevõtte ülemaailmsest aastakäibest (sõltuvalt kumb on suurem)
  2) Nö raskemad rikkumised – kuni 20 miljonit eurot või kuni 4% ettevõtte ülemaailmsest aastakäibest
- Eestis väärteomenetlus

Andmesubjekti kaebeõigus – õigus tõhusale õiguskaitsele

- Õigus esitada kaebus järelevalveasutusele, kui ta leiab, et tema andmekaitsealaseid õigusi on rikutud
- Õigus pöörduda kohtusse järelevalveasutuse tegevuse või otsuse peale
- Õigus pöörduda kohtusse vastutava või volitatud töötleja vastu, kui ta leiab, et tema andmekaitsealaseid õigusi on rikutud
- Õigus nõuda vastutavalt töötlejalt või volitatud töötlejalt andmekaitsealaste õiguste rikkumisega põhjustatud materiaalse ja mittemateriaalse kahju hüvitamist

TGS BALTIC
VARUL GRUNTE SUTKIENE

Tänud kuulamast ja kaasa mõtlemast!

Ingeri Luik-Tamme
Vandeadvokaat

ingeri.luik-tamme@tgsbaltic.com