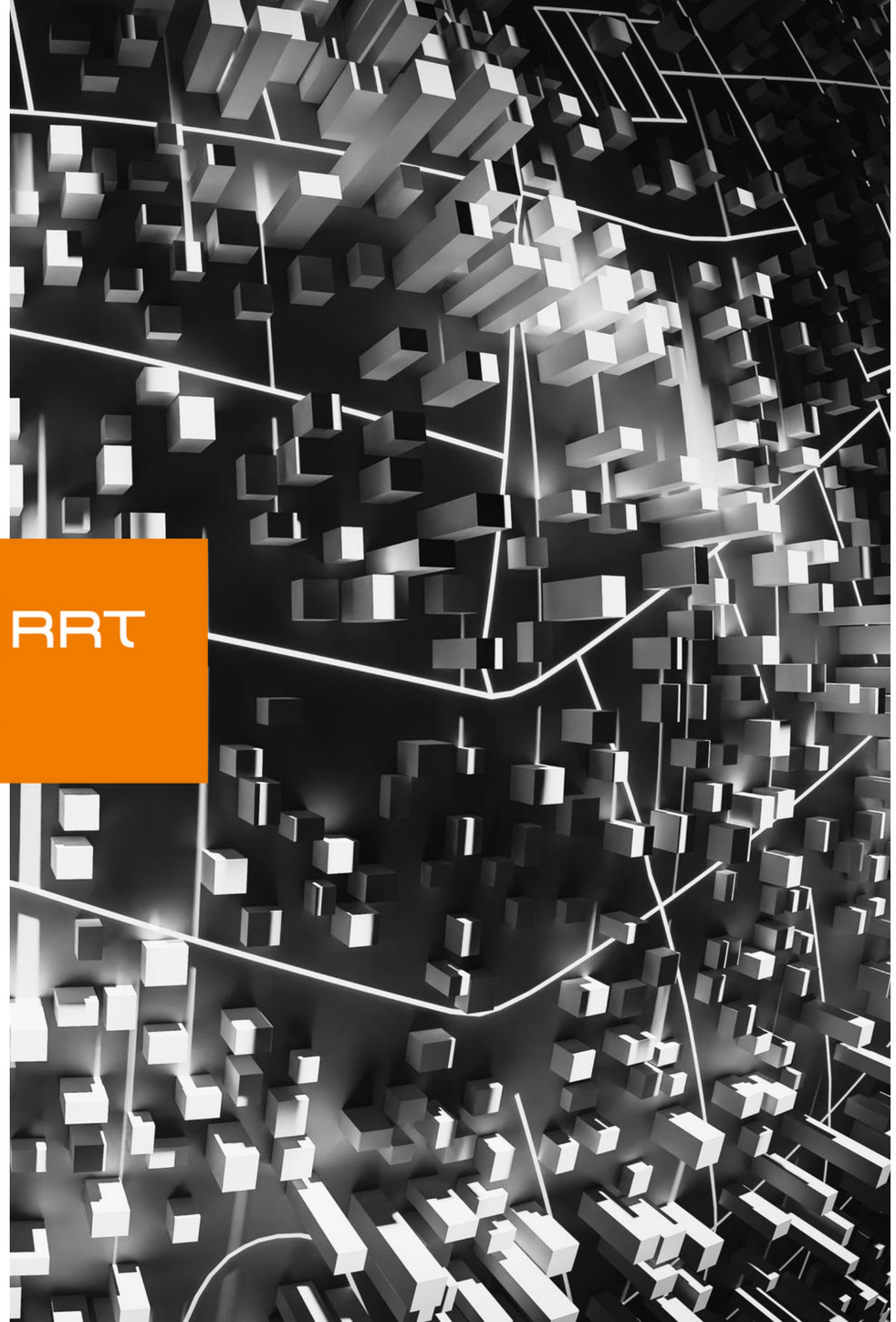

RAUDONOS LINIJOS IR GEROSIOSIOS PRAKTIKOS:
kaip užtikrinti asmens duomenų apsaugą diegiant DI

Lietuvos Respublikos ryšių reguliavimo tarnyba
Ernesta VAGONIENĖ
Skaitmeninių paslaugų reguliavimo grupės
vyriausioji patarėja

DI aktas

Tikslas – skatinti į žmogų orientuoto ir patikimo DI vystymą, kartu užtikrinant aukšto lygio sveikatos, saugumo ir pagrindinių teisių apsaugą nuo žalingo DI sistemų poveikio

DRAUDŽIAMOS DI PRAKTIKOS

- Manipuliavimo ir apgaulės metodai
- Pažeidžiamų grupių išnaudojimas
- Socialinis reitingavimas
- Individualus rizikos vertinimas
- Netikslinis veido vaizdų rinkimas
- Emocijų atpažinimas
- Biometrinis kategorizavimas
- Tikralaikis NBTN teisėsaugos tikslais

IŠIMTYS

- Nacionalinis saugumas, gynyba, kariniai tikslai
- Teisminis bendradarbiavimas su trečiosiomis šalimis
- Moksliniai tyrimai ir plėtra
- Asmeninė neprofesinė veikla
- Nemokamos ir atvirojo kodo licencijos

MANIPULIAVIMAS IR APGAULĖ

DI sistemos, kuriose pasitelkiant pasąmonę veikiančius metodus, kurių asmuo nesuvokia, arba tikslingai pasitelkiant manipuliavimo ar apgaulės metodus yra siekiama iškreipti elgesį arba pasiekiamas elgesio iškreipimas ir taip padaroma didelė žala arba yra pagrįstai tikėtina, kad didelė žala bus padaryta

ŽALINGAS PAŽEIDŽIAMUMO IŠNAUDOJIMAS

Išnaudojamas pažeidžiamumas dėl amžiaus, negalios ar konkrečios socialinės ar ekonominės padėties

SOCIALINIS REITINGAVIMAS

DI sistemos, kuriose fiziniai asmenys ar asmenų grupės vertinami ar klasifikuojami pagal jų socialinį elgesį arba asmeninius ar asmenybės bruožus ir taip nustatytas socialinis reitingas lemia žalingą ar nepalankų elgesį su asmenimis, kai duomenys yra gauti iš nesusijusio socialinio konteksto, arba toks elgesys su asmenimis yra nepagrįstas ar neproporcingas jų socialiniam elgesiui

IŠIMTYS

- Juridinių asmenų reitingavimas
- Teisėtas ir konkretus tikslas

NUSIKALSTAMOS VEIKOS VERTINIMAS

DI sistemos, kuriose, remiantis vien profiliavimu ar asmenybės bruožais ir savybėmis, vertinama arba prognozuojama rizika, kad asmenys įvykdys nusikalstamą veiką

IŠIMTYS

- Žmogaus atliekamas vertinimas, pagrįstas objektyviais ir patikrinamais faktais
- Lokalizuotas ar geoerdvinis prognozavimas
- Juridinių asmenų vertinimas
- Administracinių nusižengimų prognozės

NETIKSLINIS VEIDO ATVAIZDŲ RINKIMAS

DI sistemos, kuriomis netikslingai renkant veido atvaizdus iš interneto ar iš apsauginių vaizdo stebėjimo sistemų (AVSS) įrašų yra kuriamos arba plėtojamos veido atpažinimo duomenų bazės

IŠIMTYS

- Tikslinis rinkimas
- Netikslinis biometrinių duomenų rinkimas
- Bazės, nenaudojamos asmenims atpažinti

EMOCIJŲ ATPAŽINIMAS

DI sistemos, naudojamos emocijoms darbo vietoje ar švietimo įstaigose numanyti

IŠIMTYS

- Fizinė būklė (skausmas ar nuovargis)
- Dėl medicininių ar saugos priežasčių
- Remiamasi ne biometriniais duomenimis
- Minios valdymas

BIOMETRINIS KATEGORIZAVIMAS

DI sistemos, kuriose asmenys pagal jų biometrinius duomenis skirstomi į kategorijas siekiant nustatyti ar numanyti jų:

- rasę
- politines pažiūras
- narystę profesinėse sąjungose
- religinius ar filosofinius įsitikinimus
- lytinį gyvenimą
- seksualinę orientaciją

IŠIMTYS

- Kitai komercinei veiklai
- Būtina dėl objektyvių techninių priežasčių
- Teisėtai įgytų biometrinių duomenų rinkinių ženklinimas ar filtravimas, įskaitant teisėsaugos srityje

TIKRALAIKIS NBTN

DI sistemos, kuriose teisėsaugos tikslais naudojamas tikralaikis nuotolinis biometrinis tapatybės nustatymas viešosiose erdvėse

IŠIMTYS

- Tikslinei konkrečių nukentėjusių asmenų paieškai
- Konkrečių grėsmių, įskaitant teroristinius išpuolius, prevencijai
- Asmenų, įtariamų įvykdžiusių konkrečias nusikalstamas veikas, paieškai
- Biometrinis sutikrinimas

NUO KO PRADĖTI?

DIA reikalavimai dėl saugumo

- **Duomenų kokybė**: tikslumas, teisėtumas, reprezentatyvumas
- **Įrašų tvarkymas**: *log'ų* rinkimas audito ir atsekamumo tikslais
- **Atsparumo testavimas**: DI sistemos testai prieš diegimą
- **Kibernetinis saugumas**: apsaugos priemonės nuo nutekėjimų ir atakų.

Praktinis akcentas: tai, kas BDAR kontekste laikyta *gerąja praktika* (pseudonimizacija, šifravimas, prieigos kontrolė), pagal DIA tampa **teisiniu reikalavimu** didelės rizikos sistemoms

NEPAMIRŠTI

Duomenų valdytojo / tvarkytojo atsakomybė pagal DIA

- Užtikrinti, kad į sistemą pateikiami duomenys yra tinkami
- Prižiūrėti sistemos veikimą (ne „įdiegti ir pamiršti“)
- Imtis veiksmų nustačius rizikas (sustabdyti, koreguoti naudojimą)

Tai papildo BDAR **atskaitomybės principą** – organizacija turės įrodyti, kad laikosi abiejų reglamentų.

PIRMIAUSIA KLIENTAS

Skaidrumas ir informavimas

DIA: informuoti, jei žmogus bendrauja su DI arba jo duomenys naudojami automatizuotam sprendimui
BDAR: 13–14 str. pareiga aiškiai paaiškinti duomenų tvarkymą

Praktinis ryšys: informacijos pranešimas turi būti papildytas nuoroda į DI naudojimą

OPTIMIZACIJA

Poveikio vertinimai

BDAR: poveikio duomenų apsaugai vertinimas
DIA: poveikio pagrindinėms teisėms vertinimas

- Praktinis patarimas: **sujungti abu procesus** į vieną integruotą vertinimą

Techninės priemonės kaip jungiamoji grandis

Pseudonimizacija, šifravimas, prieigos kontrolė, auditai
Šios priemonės užtikrina atitiktį ir apsaugo organizaciją nuo atsakomybės

- Investicija tarnauja „dvigubai“

RRT

www.rrt.lt

Ryšių reguliavimo tarnyba

RRT | The Communications Regulatory Authority of the Republic of Lithuania