TECHNOLOGINĖS NAUJOVĖS IR JŲ POVEIKIS DUOMENŲ APSAUGAI

MARIUS LAURINAITIS

APIE „SolPriPa 2 WORK“ PROJEKTĄ

2021–2023 m. Valstybinė duomenų apsaugos inspekcija kartu su Mykolo Romerio universitetu įgyvendina „SolPriPa 2 WORK“ projektą „Sprendžiant privatumo paradoksą 2: aukštų duomenų apsaugos, kaip pagrindinės teisės, standartų skatinimas darbo vietoje“. Dvejų metų trukmės projektas iš dalies finansuojamas pagal Europos Sąjungos Teisių, lygybės ir pilietiškumo programą (2014–2020). Tai darbdavių ir darbuotojų informuotumo didinimo projektas apie asmens duomenų apsaugą darbo santykių kontekste.

Projekto tikslai:
1. Suteikti galimybę **darbdaviams** kurti asmens duomenų tvarkymo principus atitinkančią darbo aplinką.
2. Padėti **darbuotojams** ginti savo teisę į asmens duomenų apsaugą, kaip pagrindinę teisę, darbo vietoje.

Tikslinės auditorijos – darbuotojai, kurie yra silpnesnė darbo santykių šalis, ir darbdaviai, ypač tokie specialistai kaip duomenų apsaugos pareigūnai, personalo, komunikacijos, informacinių technologijų specialistai, kiti administracijų darbuotojai. Projekto metu numatyta didelį dėmesį skirti smulkiojo ir vidutinio verslo įmonėms, taip pat viešojo sektoriaus organizacijoms, tokioms kaip ministerijos ir joms pavaldžios institucijos, savivaldybės, teismai.

Veiklos. Įgyvendinant projektą vesti mokymai, parengtos gairės, moksliniai straipsniai, tinklalaidės, toliau vystoma mobilioji aplikacija „ADA gidas“.

Aktualios nuorodos

Projekto informacija internete (https://vdai.lrv.lt/lt/naudinga-informacija/solpripa-2-work-projektas)

Mobilioji aplikacija „ADA gidas“ (https://vdai.lrv.lt/lt/naujienos/ada-gidas-mobilioji-programele-skirta-informacijos-sklaidai-apie-asmens-duomenu-apsauga)

„SolPriPa 2 WORK“ projektas iš dalies finansuojamas pagal Europos Sąjungos Teisių, lygybės ir pilietiškumo programą (2014–2020).

PROJEKTO PARTNERIAI

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Mykolo Romerio universitetas

TECHNOLOGINĖS NAUJOVĖS

Technologinės naujovės turi ir gali padėti apsaugoti asmeninius duomenis nuo neteisėto panaudojimo ar pavojaus. Tačiau jos taip pat gali sukelti naujas duomenų saugumo rizikas. Reikia nuolat stebėti ir atnaujinti duomenų saugos strategijas, kad būtų užtikrinta, kad asmeniniai duomenys yra saugiai ir teisėtai tvarkomi.

DIRBTINIS INTELEKTAS. EUROPOS POŽIŪRIS.

Dirbtinis intelektas (DI) sparčiai tobulėja. Jis pakeis mūsų gyvenimą, padėdamas užtikrinti geresnę sveikatos priežiūrą (pvz., tikslesnį diagnozavimą ir geresnę ligų prevenciją), efektyviau ūkininkauti, švelninti klimato kaitą ir prisitaikyti prie jos, didinti gamybos sistemų veiksmingumą dėl prognozuojamosios priežiūros, didinti europiečių saugumą ir įvairiais kitais būdais, kuriuos kol kas menkai įsivaizduojame. Kartu DI gali atnešti nemažai pavojų, tokių kaip neskaidrus sprendimų priėmimas, diskriminacija dėl lyties arba kitų veiksnių, brovimasis į privačią erdvę arba naudojimas nusikalstamais tikslais.

DIRBTINIS INTELEKTAS

- nauja nauda piliečiams, pavyzdžiui, geresnė sveikatos priežiūra, mažiau gendanti buities įranga, saugesnio ir švaresnio transporto sistemos, geresnės viešosios paslaugos;
- plėtros galimybės verslui, pavyzdžiui, naujos kartos produktai ir paslaugos tose srityse, kuriose Europa yra ypač stipri (mašinos, transportas, kibernetinis saugumas, ūkininkavimas, žalioji ir žiedinė ekonomika, sveikatos priežiūra ir didelės pridėtinės vertės sektoriai, pvz., mada ir turizmas),
- viešojo intereso paslaugas teikiantiems subjektams, pavyzdžiui, mažesnė (transporto, švietimo, energetikos ir atliekų tvarkymo) paslaugų teikimo kaina, didesnis produktų tvarumas ir tinkamos priemonės teisėsaugos institucijoms piliečių saugumui užtikrinti, kartu taikant tinkamas priemones jų teisėms ir laisvėms apsaugoti.

DIRBTINIS INTELEKTAS

- PRAMONĖS IR PROFESINIŲ RINKŲ PRANAŠUMŲ IŠNAUDOJIMAS.
- ATEITIES GALIMYBIŲ IŠNAUDOJIMAS. KITA DUOMENŲ BANGA.
- KOMPETENCIJOS EKOSISTEMA.
- **MOKSLO IR INOVACIJŲ BENDRUOMENĖS PASTANGŲ TELKIMAS.**
- PASITIKĖJIMO EKOSISTEMA DI REGLAMENTAVIMO SISTEMA.

DIRBTINIS INTELEKTAS

- Galimas nerimas dėl:
  - Pagrindinėms teisėms, įskaitant teisę į asmens duomenų bei privatumo apsaugą ir nediskriminavimą, kylanti rizika.
    - Žmogus, priimdamas sprendimus, nėra apsaugotas nuo klaidų ir neobjektyvumo. Tačiau DI neobjektyvumo padariniai galėtų būti kur kas didesni, dėl jo gali nukentėti ir būti diskriminuojami daug žmonių, nes nėra socialinės kontrolės mechanizmų, reguliuojančių žmonių elgesį.
  - Pavojus saugai ir veiksmingam atsakomybės užtikrinimui.
    - Pagal Atsakomybės už gaminius direktyvą už žalą dėl gaminio trūkumų atsako gamintojas. Tačiau DI sistemų, kaip antai savivaldžių automobilių, atveju gali būti sunku įrodyti, jog gaminys turi trūkumų, buvo padaryta žala ir tarp šių dviejų dalykų yra priežastinis ryšys. Be to, neaišku, kaip ir kokiu mastu Atsakomybės už gaminius direktyva taikoma tam tikrų rūšių trūkumams, pavyzdžiui, jei jų atsiranda dėl gaminio kibernetinio saugumo spragų.

DIRBTINIS INTELEKTAS

DI gali kelti grėsmes asmens duomenų apsaugai keliais būdais:

- šnipinėjimas: DI algoritmai gali būti naudojami neteisėtai gauti prieigą prie asmeninių duomenų.
- analizė: DI algoritmai gali būti naudojami neteisėtai analizuoti asmeninius duomenis ir ištraukti jų asmeninę informaciją.
- paskirstymas: paskirstyti asmeninius duomenis be asmens sutikimo.
- panaudojimas: DI algoritmai gali būti naudojami neteisėtai panaudoti asmeninius duomenis (politiniams ar ekonominiams tikslams).

DAIKTŲ INTERNETAS

(IoT) gali kelti grėsmes asmens duomenų apsaugai keliais būdais:

- Pažeidžiamumas įrenginiuose: IoT įrenginiai gali būti pažeidžiami dėl neatsparių saugos mechanizmų, leidžiančių neteisėtai gauti prieigą prie asmeninių duomenų.
- Duomenų perdavimas: IoT įrenginiai gali automatiškai perduoti asmeninius duomenis į trečiųjų šalių serverius, be asmens sutikimo ar žinios.
- Duomenų analizė: IoT įrenginiai gali būti naudojami neteisėtai analizuoti asmeninius duomenis ir ištraukti jų asmeninę informaciją.
- Automatinis paskirstymas: IoT įrenginiai gali automatiškai paskirstyti asmeninius duomenis, pavyzdžiui, per skelbimų ar reklamos sistemas, be asmens sutikimo.
- Duomenų panaudojimas: IoT įrenginiai gali būti naudojami neteisėtai panaudoti asmeninius duomenis, pavyzdžiui, politiniams ar ekonominiams tikslams.

AČIŪ