PATVIRTINTA
Greitosios medicinos pagalbos
tarnybos generalinio direktoriaus
2025 m. gegužės 30 d.
įsakymu Nr. V-212

REKOMENDACIJOS, KAI GREITOSIOS MEDICINOS PAGALBOS TARNYBOJE, DIRBTINIO INTELEKTO TECHNOLOGIJŲ SPRENDIMAMS BŪTINI ASMENS DUOMENYS

Darbuotojai prieš pradėdami naudoti Greitosios medicinos pagalbos tarnyboje (toliau – Tarnyba) dirbtinio intelekto (toliau – DI) sistemas turi:

1. Susipažinti:

1.1. su pačia DI sistema, įvertinti, kas yra DI sistemos paslaugų teikėjas;

1.2. su sistemos aprašymu, funkcionalumais, naudojimo taisyklėmis ar kitais pasiekiamais dokumentais (pavyzdžiui, privatumo politika, taikomų saugumo priemonių aprašymas ar nuorodos į taikomus saugumo standartus, turimus sertifikatus, kt.);

1.3. ir žinoti, kaip ši sistema veiks: kokie ir kaip duomenys bus naudojami, kokie yra duomenų šaltiniai (pavyzdžiui, ar bus naudojami tik tokie duomenys, kuriuos Tarnyba šiai sistemai pateiks jos apmokymui ar apdorojimui, ar šie duomenys bus renkami iš kitų šaltinių ir pan.);

1.4. ir nustatyti, ar DI sistemos veikimui būtini asmens duomenys.

2. Nustačius, kad **asmens duomenys**, naudojant DI sistemą, bus tvarkomi, tuomet rekomenduojama vadovautis toliau nurodytais (minimaliais) žingsniais:

2.1. **1 žingsnis,** nustatyti DI sistemos naudojimo tikslą, įvertinus galimas rizikas, kibernetinės saugos reikalavimus, bei atsižvelgus į BDAR įtvirtintas teises duomenų subjektams. Įvertinti kaip DI sistemos funkcionalumai yra suderinami su siekiamu jos naudojimo tikslu Tarnyboje ir pasirinktomis rizikos valdymo priemonėmis.

Pavyzdžiui, jei DI sistemos naudojimo tikslas yra priimti žmonių atžvilgiu automatizuotus sprendimus, reikėtų įvertinti, ar tokia sistema sudaro sąlygas pateikti tokiam žmogui prasmingą informaciją apie loginį priimto sprendimo pagrindimą (kaip tai reikalaujama pagal BDAR 15 straipsnio 1 dalies h punktą.

2.2. **2 žingsnis,** nustatyti, kokį statusą (duomenų valdytojas ar (ir) (duomenų tvarkytojas) turės tvarkant asmens duomenis tokia DI sistema. Naudojimo etape, kai tokiu būdu bus tvarkomi asmens duomenys, Tarnyba bus duomenų valdytoją, nes Tarnyba nustatys asmens duomenų tvarkymo tikslus ir esmines priemones.

Esminių priemonių nustatymas reiškia, kad Tarnyba pasirenka, kieno ir kokie asmens duomenys yra būtini konkrečiam tikslui pasiekti, jų tvarkymo trukmę, duomenų gavėjų kategorijas, o taip pat pasirenka konkrečią programinę įrangą tokiam tvarkymui. Tais atvejais, kai minėtus sprendimus priima kelios įstaigos, jos gali būti laikomos bendrais duomenų valdytojais.

Pavyzdžiui, būti kelių ligoninių bendras sprendimas pasitelkti DI sistemą, siekiant padėti gydytojams įvertinti pacientų anamnezes ir nustatyti taikytiną gydymą.

2.3. **3 žingsnis,** nustatyti asmens duomenų tvarkymo teisinį pagrindą (ir, kai taikoma, atlikti vadovaujantis Tarnybos generalinio direktoriaus įsakymu patvirtintomis asmens Teisėto intereso pusiausvyros (balanso) atlikimo testo, tvarkant asmens duomenis, taisyklėmis. Svarbu, nuo DI sistemos gyvavimo ciklo etapo (apmokymo, naudojimo ar tobulinimo (angl. development, deployment, fine-tuning), teisiniai pagrindai gali būti skirtingi.

Pavyzdžiui, priklausomai nuo DI sistemos, jos kūrimo procese asmens duomenų tvarkymas tam tikrais atvejais galėtų būti grindžiamas Tarnybos teisėtu interesu, o šios sistemos naudojimas gali būti paremtas asmens sutikimu.

Pavyzdžiui, pareigą atlikti interesų balanso vertinimą, būtina kiekviename etape, kuriame DI sistema bus pasitelkta, vertinti atskirai. Taip pat būtina įvertinti ir tai, ar asmens duomenys bus gauti tiesiogiai iš žmogaus (jei ne, reikėtų itin kruopščiai įvertinti, ar iš kitų šaltinių gautų duomenų naudojimas DI sistemų pagalba atitiktų teisėtumo reikalavimus). Siekiant jau tvarkomus asmens duomenis tvarkyti nauju tikslu (t. y. asmens duomenų tvarkymo veikla, dėl kurios asmens duomenys buvo surinkti, ir veikla, kuriai asmens duomenys bus tvarkomi panaudojant DI sistemą, nesutampa), turi būti nustatyta, ar tikrai yra teisinis pagrindas naujai asmens duomenų tvarkymo veiklai. Tuo atveju, jei asmens duomenų tvarkymo veiklos tikslas išlieka tas pas, bet joje pradedama naudoti (svarstoma naudoti) DI sistema, turi būti įvertinta ir tai, ar tokiu būdu asmens duomenis tvarkyti galima pagal BDAR 6 straipsnio 4 dalį.

2.4. **4 žingsnis,** nustatyti, kokie asmens duomenys yra būtini svarstomos DI sistemos naudojimo kontekste. Įvertinti ar asmens duomenys tikrai būtini ir ar visuose DI sistemos etapuose reikia asmens duomenų atskirai. Įvertinti visas asmens duomenų tvarkymo aplinkybes ir ar asmens duomenys tvarkomi suderinamu tikslu.

Kai DI sistemos apmokymui ar naudojimui naudojami duomenų valdytojo tvarkomi asmens duomenys, duomenų valdytojas turi atlikti ir šių asmens duomenų tvarkymo tikslo suderinamumo vertinimą (įvertinant tai, kad šiuo atveju išimtys, kai tokio vertinimo nereikia atlikti, nebus taikomos), kaip tai numatyta BDAR 6 straipsnio 4 dalyje. Jei siekiamą tikslą galima pasiekti be asmens duomenų, tokiam sprendimui turėtų būti teikiama pirmenybė, o jei asmens duomenis tvarkyti būtina, turi būti užtikrinta, kad bus tvarkoma tik minimaliai būtina jų apimtis.

2.5. **5 žingsnis**, nustatyti**,** kokią riziką asmenims (kurių asmens duomenis tvarkysite) gali sukelti svarstomos DI sistemos kūrimas ar naudojimas. BDAR įtvirtintas atskaitomybės principas įpareigoja duomenų valdytoją ne tik laikytis su asmens duomenų apsauga susijusių principų, bet ir imtis tinkamų organizacinių ir techninių priemonių, siekiant užtikrinti (ir įrodyti), kad šių principų yra laikomasi (BDAR 5 straipsnio 2 dalis ir 24 straipsnis). BDAR 25 ir 32 straipsniai įpareigoja duomenų valdytoją, vertinant, kokias organizacines ir technines saugumo priemones būtina pasirinkti, atsižvelgti į tam tikrus kriterijus, kitaip tariant – atlikti rizikos vertinimą (vertinant kartu su BDAR 5 straipsnio 2 dalimi, būtina tai dokumentuoti) ir, priklausomai nuo gauto rezultato, pasirinkti tinkamas organizacines ir technines priemones.

Dalis tokių priemonių yra susijusios su saugumo politikos, prieigos kontrolės politikos, informacinių technologijų keitimų valdymo politikos, reagavimo į saugumo incidentus

plano, saugumo incidentų likvidavimo plano, asmens duomenų šifravimo tvarkos ir t. t. Rizikos vertinimą būtina atlikti visais atvejais, kai siekiama tvarkyti asmens duomenis. Priklausomai nuo naudojamos DI sistemos ir jos apmokymui ar naudojimui būtinų asmens duomenų, atskirais atvejais gali būti aktualu atlikti poveikio duomenų apsaugai vertinimą (PDAV). Ši pareiga taikoma tais atvejais, kai dėl numatomo asmens duomenų tvarkymo žmogaus teisėms ir laisvėms gali kilti didelis pavojus (BDAR 35 straipsnis).

2.6. **6 žingsnis,** nustatyti Nustatykite, ar ir kaip tvarkant asmens duomenis kuriant ar naudojant DI sistemą įgyvendinsite duomenų subjektų teises.

Tais atvejais, kai DI sistemos vystymui, naudojimui ar tobulinimui tvarkomi asmens duomenys, būtina užtikrinti, kad duomenų subjektų teisės būtų įgyvendinamos**: t**eisė būti informuotam, teisė būti pamirštam, teisė prieštarauti ir pan.

Teikiant informaciją duomenų subjektams, nurodoma, kad konkrečiam duomenų tvarkymui yra / bus naudojama DI sistema, taip pat kokie asmens duomenys ir kaip bus tvarkomi panaudojant DI sistemą, kokią įtaką (poveikį) tai turės patiems duomenų subjektams.

BDAR nenustato konkrečių būdų, kaip informuoti duomenų subjektus, primintina, kad pasirinktas būdas turi sudaryti sąlygas duomenų subjektui suprasti, kad jo asmens duomenys bus tvarkomi DI sistemos veikimo kontekste prieš tai, kai pateikia savo asmens duomenis.

2.7. **7 žingsnis,** kreiptis į specialistus (duomenų apsaugos pareigūną (DAP), saugos įgaliotinį, išorės ar vidinius ekspertus ir kt.) dėl DI sistemos rizikų, naudojimo specifikos, susijusių pareigų ar pan.

DAP turi būti savalaikiai įtrauktas į visus pasitarimus ar kitas veiklas, kai svarstomi / priimami sprendimai, susiję su asmens duomenų tvarkymu Tarnybos (duomenų valdytojo) veikloje (BDAR 38 straipsnio 1 dalis). Tuo atveju, jei priimamas sprendimas DAP nuomone nesiremti, tokį sprendimą rekomenduojama dokumentuoti.

Rekomendacijose nustatyti minimalūs reikalavimai pasitelkiant DI sistemas. Darbuotojai ar duomenų valdytojai ketinantys naudoti savo darbe DI sistemas įgyvendindami atskaitomybės principą, turi įvertinti, kokie kiti reikalavimai jiems taikomi ir užtikrinti, kad jų būtų laikomasi.

Rekomendacijos parengtos atsižvelgiant į Valstybinės duomenų apsaugos inspekcijos pateiktą informaciją šioje nuorodoje:

https://vdai.lrv.lt/public/canonical/1748518193/944/2025-05-29%20DUK%20del%20DI%20sprendimu_galutinis2.pdf

_____