VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

REKOMENDACIJOS DĖL ASMENS TAPATYBĖS NUSTATYMO INTERNETE

PARENGTOS PAGAL DARBO GRUPĖS ASMENŲ APSAUGAI REKOMENDACIJĄ WP 68 „DARBO DOKUMENTAS DĖL TAPATYBĖS NUSTATYMO PASLAUGŲ INTERNETE“

PRATARMĖ

Europos Sąjungos Komisija jau 1997–1998 m. pranešimuose akcentavo interneto (on- line) aplinkos keliamus pavojus asmens duomenų apsaugai. Interneto (on-line) aplinkai būdinga veikėjų gausa, labai spartūs struktūros ir formos pokyčiai, naujausi informacijos tvarkymo būdai, teritorinio apribojimo nepaisymas, tarpkontinentinė struktūra. Paieškos sistemos, slapukai, virtualios parduotuvės, elektroniniai atsiskaitymai, žaidimai – tai tik keletas Interneto paslaugų pavyzdžių. Jos visos pasižymi potencialia galimybe itin greitai ir efektyviai rinkti ir platinti vartotojų duomenis.

Europos Parlamento direktyvos dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB) (toliau – Direktyva) 12 straipsnis, įtvirtina, kad valstybės narės garantuoja kiekvieno duomenų subjekto teisę reikalauti, kad duomenų valdytojas be apribojimų, priimtinais laiko tarpais, per daug nedelsdamas ir be pernelyg didelių išlaidų, pateiktų žinias apie loginius metodus, naudojamus automatiškai tvarkant duomenų subjekto asmens duomenis.

Direktyvos 2 straipsnis asmens duomenis apibrėžia kaip bet kurią informaciją, susijusią su asmeniu („duomenų subjektu”), kurio tapatybė yra nustatyta arba gali būti nustatyta tiesiogiai ir netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu, vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais požymiais.

Šiuo metu yra žinomi keturi vartotojo tapatybės nustatymo būdai:

- Slaptažodžio valdymas yra atliekamas vartotojo kompiuterio naršyklėje.
- Slaptažodžio valdymas yra atliekamas interneto paslaugų „proxy” serveryje.
- Tapatybę nustato trečia šalis, naudodama specialius tapatybės nustatymo protokolus. Tai yra realizuota Microsoft NET Passport sistemoje, kuri teikia asmens tapatybės nustatymo paslaugas.
- Tapatybę nustato šalis, kuri yra viena iš pasitikėjimo grupės narių, susijusių tarpusavio susitarimais. Čia naudojamas specifinis protokolas, pvz., vienas iš „Liberty Aliance“ projektų.

I. BENDROSIOS NUOSTATOS

1. Šių Rekomendacijų paskirtis – suteikti individualiems interneto vartotojams visą reikalingą informaciją, kuri paskatintų pasitikėti interneto svetainėmis, kuriose jie lankosi, ir supažindintų su tam tikromis alternatyvomis bei su jų teisėmis, įtvirtintomis Europos Sąjungos teisėje, nepažeidžiant Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo. Jos parengtos pagal Darbo grupės asmenų apsaugai tvarkant asmens duomenis 2003 m. rekomendaciją WP 68 „Dėl tapatybės nustatymo paslaugų internete.”

2. Šių Rekomendacijų tikslas – pateikti metodinius nurodymus dėl asmens tapatybės nustatymo internete, išdėstyti minimalius reikalavimus, kuriais būtų lengva vadovautis duomenų valdytojams (fiziniams ar juridiniams asmenims, atsakingiems už asmens duomenų tvarkymą internete), valdantiems svetaines, informuoti individualius interneto vartotojus apie jų teises, kad jie galėtų priimti sprendimą prieš pasirinkdami paslaugas, kurios atitiktų vartotojo pageidaujamą lygį.

3. Rekomendacijos taikytinos asmens duomenų valdytojams, renkantiems duomenis internetu, teikiant jiems praktinius patarimus, minimalių konkrečių priemonių sąrašą, ir individualiems interneto vartotojams. Be to, šios Rekomendacijos galėtų pasitarnauti kaip metodika

kuriant tapatybės nustatymo programinę ir techninę įrangą, skirta asmens duomenų rinkimui ir tvarkymui internete, standartus.

II. MINIMALŪS REIKALAVIMAI DĖL TAPATYBĖS NUSTATYMO INTERNETE

4. Elektroninio verslo sistemos iš duomenų subjekto, t.y. vartotojo, turėtų reikalauti tik minimalios informacijos, reikalingos nustatyti vartotojo tapatybę, pvz., elektroninio pašto adreso, slaptažodžio. Papildomai gali būti pareikalauta pateikti slaptą klausimą ir slaptą atsakymą. Slaptas klausimas ir atsakymas naudojamas patikrinti vartotojo tapatybę (kad čia yra tas vartotojas). Pvz., kiekvienas NET Passport vartotojas naudoja unikalų identifikatorių, kuris sukuriamas registracijos metu ir egzistuoja visą sąskaitos gyvavimo laiką. Kur sąsaja su vartotoju yra reikalinga, tačiau nereikia pilno identifikavimo, turėtų būti siūloma naudotis pseudonimais.

5. Vartotojui turėtų būti sudaryta galimybė naudotis internete teikiamoms paslaugomis, išlaikant kuo daugiau anonimiškumo.

6. Siekiant užtikrinti sąžiningą asmens duomenų tvarkymą, tam tikra informacija turėtų būti pateikta iš karto ekrane prieš pradedant duomenų rinkimą. Tai informacija apie:

6.1. Valdytojo ir jo atstovo tapatybę, buveinės adresą bei svetainės elektroninio pašto adresą.

6.2. Tikslą (ar tikslus), kuriuo valdytojas tinklalapyje renka asmens duomenis iš vartotojo. Pavyzdžiui, kai duomenys renkami siekiant įvykdyti sutartį (paslaugų teikimas, produktų užsakymas, internetinė prenumerata) ar tiesioginės rinkodaros tikslais, valdytojas turėtų aiškiai nurodyti šiuos tikslus.

6.3. Privalomą ar neprivalomą reikalaujamos informacijos pobūdį. Privaloma informacija yra tokia, kuri būtina paslaugos išpildymui. Privalomas ar neprivalomas pobūdis galėtų būti žymimas sutartiniu ženklu, pvz., žvaigždute prie neprivalomos informacijos, pridedant prierašą „neprivaloma”. Jei duomenų subjektas nepateikia neprivalomos informacijos, tai neturėtų niekaip jam pakenkti.

6.4. Surinktų duomenų gavėjus ar gavėjų kategorijas. Renkant bet kokius duomenis, duomenų valdytojas turi nurodyti, ar surinkti duomenys bus atskleidžiami ir prieinami trečioms šalims, pvz., verslo partneriams, dukterinėms įmonėms ir pan., ir kodėl (nei tik reikalaujamos paslaugos suteikimo ar tiesioginės rinkodaros tikslais).

6.5. Asmens teisę susipažinti su surinktais duomenimis ir reikalauti juos pataisyti. Tai yra duomenų subjekto teisė turėti galimybę bet kuriuo laiku, be papildomo užmokesčio susipažinti, keisti, trinti, taisyti savo profilius internetinių paslaugų teikėjo puslapyje. Profiliuojančios tarnybos turėtų užtikrinti (on-line) tipo priėjimą prie vartotojo saugomų duomenų. Pvz., vartotojas, turėdamas Microsoft'o NET Passport sąskaitą, gali nuspręsti, teikti informaciją kitoms svetainėms ar ne, prieš tai atitinkamai pažymėdamas savo sutikimą dėl informacijos suteikimo. Jei profiliuojanti informacija yra kaupiama naudojant pseudonimus, vartotojai privalo turėti galimybę taisyti, keisti ir trinti savo duomenis anonimiškai.

6.6. Teisę nesutikti su duomenų atskleidimu trečiosioms šalims, kitais nei nurodytos paslaugos suteikimas, tikslais ir pasinaudojimo šia teise būdą. Šiuo atveju interneto vartotojai privalo turėti realią galimybę prieštarauti dėl duomenų atskleidimo internetu kitais, nei reikalaujamos paslaugos suteikimas tikslais, pvz., tai galėtų būti realizuota, paslaugos užsakymo metu, pažymint atitinkamus pasirinkimus. Galimybė realizuoti šią teisę, turi būti užtikrinta visada.

6.7. Automatines rinkimo procedūras. Pavyzdžiui, kai naudojamos tokios procedūros, duomenų subjektui turėtų būti suteikta informaciją apie duomenų saugojimo tipą, mąstą, vietą. Subjektas turėtų būti informuotas apie interneto svetainės serverio srities (domeno) vardą, kuriuo perduodamos automatinės duomenų rinkimo procedūros, tų procedūrų tikslą, jų galiojimo laiką, taip pat ar būtina sutikti su tokiomis procedūromis yra būtinas norint aplankyti svetainę, ar yra galimybė bet kuriam interneto vartotojui paprieštarauti dėl duomenų naudojimo, kokios tokių procedūrų pasekmės. Tokiais atvejais, kai kiti duomenų valdytojai yra įtraukti į asmens duomenų rinkimą,

duomenų subjektui turėtų būti suteikta informacija apie duomenų valdytojo tapatybę, kiekvieno duomenų valdytojo duomenų tvarkymo tikslai.

6.8. Saugumo lygį visuose tvarkymo etapuose. Pavyzdžiui, perduodant duomenis iš naudotojo įrangos į interneto svetainę, galima būtų patalpinti tokio pobūdžio antraštę: „Jūs įeinate į saugią sesiją" arba naudoti automatinės informacijos procedūras, esančias naršyklėje, pvz. specifinių rakto ar pakabinamos spynos formos piktogramų pasirodymas, naudojant SSL (Secure Sockets Layers) ryšio saugumą užtikrinančius protokolus. Taip pat būtų galima sumažinti autorizacijos bilieto gyvavimo laiką.

7. Visa ši informacija turėtų būti pateikta aiškiai ir lengvai suprantama vartotojui forma visomis kalbomis, kuriomis paslaugos yra siūlomos. Ši informacija galėtų būti pateikta naudojant "iššokančio" (angl. *"pop-up")* lango techniką.

8. Išsami informacija apie privatumo politiką (įskaitant būdus kaip pasinaudoti teise susipažinti su duomenimis) turėtų būti tiesiogiai pasiekiama iš pagrindinio interneto svetainės puslapio *(home page)*. Antraštė, kurią galima paspausti, turi būti pakankamai ryški, aiški, ir tiksli, leidžianti interneto vartotojui aiškiai suprasti puslapio, į kurį jis siunčiamas, pobūdį. Pavyzdžiui, antraštė gali teigti: „Mes renkame ir tvarkome jūsų asmens duomenis. Jei norite išsamesnės informacijos, spauskite čia" arba „Asmens duomenys ar privatumo apsauga". Informacijos, į kurią nukreipiamas vartotojas, turinys turi būti pakankamai aiškus. Taip pat turėtų būti pateikta privatumo politikos atnaujinimo data.

III. DUOMENŲ SUBJEKTO TEISIŲ ĮGYVENDINIMAS

9. Vartotojo privatumo labui labai svarbu kad jis, prieš duodamas sutikimą rinkti duomenis, perskaitytų kiekvienos svetainės ar tarnybos privatumo ataskaitą, kad suprastų, kaip duomenų valdytojas gali panaudoti jo asmens duomenis. Pavyzdžiui, vartotojas, besinaudojantis NET Passport paslaugomis, nusprendžia, kuria informacija bus dalinamasi su atitinkamomis svetainėmis ar duomenų valdytojais, atitinkamai tai pažymėdamas tinklo pase.

10. Internetinių paslaugų teikėjai taip pat turėtų pateikti pavadinimą ir adresą tarnybos ar asmens (buveinės ir elektroninio pašto adresą), atsakingo už atsakymus į klausimus, susijusius su asmens duomenų apsauga. Į vartotojų paklausimus ir prašymus pageidautina atsakyti vartotojo kalba.

11. Prieš užsisakant paslaugas, vartotojas turi duoti savanorišką sutikimą naudotis tomis paslaugomis. Sutikimas – savanoriškas duomenų subjekto valios pareiškimas tvarkyti jo asmens duomenis jam žinomu tikslu. (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 2 straipsnio 11dalis). Vartotojo sutikimas ar nesutikimas galėtų būti realizuotas mygtuko pagalba.

12. Vartotojas turėtų būti aiškiai informuotas, kaip pradėti paslaugų užsakymo procedūra, pvz., kaip užsisakyti tam tikras paslaugas nenaudojant savo tikrojo elektroninio pašto adreso, o naudojant anoniminį elektroninį pašto adresą.

13. Vartotojas turėtų būti aiškiai informuotas, kaip atsisakyti paslaugų teikėjo teikiamos paslaugos. Pvz., vartotojas individualią sąskaitą galėtų uždaryti vadovaudamasis „žingsnio" nurodymais, taip pat vartotojas galėtų būti supažindintas su puslapiu, kuriame būtų aprašoma sąskaitos uždarymo svarba, ir pateikiami mygtukai sąskaitos uždarymui.

14. Vartotojas privalo turėti galimybę atsisakyti neprašytų reklaminių pranešimų naudodamas filtravimo priemones. Pavyzdžiui, elektroninio pašto filtrai atliktų ateinančių elektroninio pašto žinučių filtravimą ir praleistų tik tas, kurias vartotojas nurodė kaip pageidaujamas.

15. Svetainės turėtų jungtis TRUSTe, Privaseek, Better Business Bureau, WebTrust ar panašiais privatumo saugos ženklais, t.y. konfidencialumo žymės suteikiamos svetainėms, kurios atitinka visus reikalavimus, numatytus žymėjimo organizacijos. Pavyzdžiui, organizacija gali

vykdyti tam tikro pobūdžio kontrolę, ar kompanijos, turinčios tokias žymes, laikosi jų skelbiamos konfidencialumo politikos, atlikdama reguliarius tokių kompanijų veiklos patikrinimus.

16. Internetinių paslaugų tarnybos turėtų informuoti vartotojus dėl slapukų naudojimo vartotojų profiliams sudaryti. Pavyzdžiui, jei slapukas (cookie) yra valdytojo serveryje, informacija turėtų būti suteikta prieš tai, kai ji persiunčiama į interneto naudotojo kietąjį diską. Dabartinės Microsoft'o NET Passport ir „Liberty Aliance“ tapatybės nustatymo sistemos naudoja autentifikavimo protokolus su slapukais.

17. Informacija ir prieštaravimo dėl rinkimo galimybė turėtų būti nurodyta prieš naudojant bet kokias automatizuotas procedūras, kurios leidžia vartotojo kompiuteriui susisiekti su kita svetaine, pvz., kai vartotojas automatiškai vedamas vienos svetainės į kitą, kad peržiūrėtų reklamą „banerių” (reklaminių juostelių) pavidalu, panaikinant galimybę antrajai svetainei rinkti duomenis be vartotojo žinios.

18. Kai informacija perduodama į trečią šalį, kurioje negarantuojamas adekvatus duomenų apsaugos lygis, duomenų valdytojas turėtų užtikrinti, kad duomenų perdavimas įvyktų laikantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo toliau Žin., 1996, Nr. 63-1479; 2003, Nr. 15-597) 28 straipsnio 3 dalies. Tokiais atvejais būtina informuoti vartotoją apie adekvačias garantijas, siekiant perdavimą padaryti teisėtu.

19. Interneto svetainės, kurios apdoroja elektroninius sandorius, turi korektiškai save autentifikuoti, t.y. pateikti įrodymus, kad jos yra tas kuo ir skelbiasi esančios (pvz., “elektroniniai sertifikatai”).

20. Elektroninių operacijų metu turėtų būti renkami tik tie asmens duomenys, kurie yra būtini operacijoms atlikti.

21. Elektroninių operacijų atlikimo metu turėtų būti naudojamos šifravimo technologijos sandorio konfidencialumo ir vientisumo užtikrinimui.

IV. SAUGUMO PRIEMONĖS

22. Saugumo politika turėtų apimti administracines, technines ir fizines saugumo priemones, įskaitant tikslinamą saugumo politiką, besiremiančia LST ISO/IEC 17799: 2002 standartu. Standartinės darbo procedūros turėtų būti modifikuotos, kad užtikrintų informacijos saugumo programos laikymąsi. Šios procedūros turėtų būti nuolat atnaujinamos ryšium su technologijos ir verslo vystymusi.

23. Turi būti paskirtas darbuotojas ar darbuotojai, kurie koordinuotų ir būtų atsakingi už informacijos saugumo programos įgyvendinimą. Ši programa galėtų apimti: darbo saugumo mokymą, reagavimą į incidentus ir procedūrų taikymą, saugumo priežiūros grupės sukūrimą.

Parengė:
Valstybinės duomenų apsaugos inspekcijos
Registro IT ir ryšių skyriaus vyr. specialistas (telekomunikacijų)
Zigmantas Medutis
2003-07-25

Atnaujino:
Valstybinės duomenų apsaugos inspekcijos
Informacijos ir technologijų vyr. specialistas
Zigmantas Medutis
2005-04-19