II

(Įstatymo galios neturintys teisės aktai)

REGLAMENTAI

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) Nr. 1179/2011

2011 m. lapkričio 17 d.

kuriuo pagal Europos Parlamento ir Tarybos reglamentą (ES) Nr. 211/2011 dėl piliečių iniciatyvos nustatomos internetinių pritarimo pareiškimų rinkimo sistemų techninės specifikacijos

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 211/2011 dėl piliečių iniciatyvos [1], ypač į jo 6 straipsnio 5 dalį,

pasikonsultavusi su Europos duomenų apsaugos priežiūros pareigūnu,

kadangi:

(1) Reglamente (ES) Nr. 211/2011 nustatyta, kad tais atvejais, kai pritarimo pareiškimai renkami internetu, tam tikslui naudojama sistema turi atitikti tam tikrus saugumo ir techninius reikalavimus ir turi būti sertifikuota atitinkamos valstybės narės kompetentingos institucijos;

(2) internetinė pritarimo pareiškimų rinkimo sistema, kaip apibrėžta Reglamente (ES) Nr. 211/2011, yra informacinė sistema, sudaryta iš programinės įrangos, aparatinės įrangos, prieglobos aplinkos, veiklos procesų ir darbuotojų, reikalingų atlikti pritarimo pareiškimų surinkimą internetu;

(3) Reglamente (ES) Nr. 211/2011 nustatyti reikalavimai, kuriuos internetinės pritarimo pareiškimų rinkimo sistemos turi atitikti, kad jas būtų galima sertifikuoti, ir nustatyta, kad Komisija turėtų priimti specialias šių reikalavimų įgyvendinimo specifikacijas;

(4) Atvirųjų internetinių taikomųjų programų saugumo projekto (angl. OWASP) 2010 m. dokumente „Top 10“ pateikta internetinių taikomųjų programų didžiausios saugumo rizikos ir jos mažinimo priemonių apžvalga; todėl techninės specifikacijos parengtos remiantis šio projekto išvadomis;

(5) organizatorių įgyvendinamomis techninėmis specifikacijomis turėtų būti užtikrinta, kad valstybių narių valdžios institucijos sertifikuotų internetines pritarimo pareiškimų rinkimo sistemas ir prisidėtų prie to, kad būtų imtasi reikiamų techninių ir organizacinių priemonių, būtinų tam, kad Europos Parlamento ir Tarybos direktyva 95/46/EB [2] nustatytų duomenų tvarkymo veiklos saugumo įpareigojimų būtų laikomasi ir projektuojant duomenų tvarkymo sistemą, ir tvarkant duomenis, kad užtikrinus saugumą nebūtų galima duomenų tvarkyti be leidimo, o asmens duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo arba nuo atsitiktinio praradimo, pakeitimo, neleistino atskleidimo ar prieigos;

(6) patvirtinimo procesas turėtų būti lengvesnis dėl organizatorių naudojamos programinės įrangos, kurią pagal Reglamento (ES) Nr. 211/2011 6 straipsnio 2 dalį parengė Komisija;

(7) piliečių iniciatyvų organizatoriai, kaip duomenų valdytojai, internetu rinkdami pritarimo pareiškimus turėtų laikytis šiame reglamente nustatytų techninių specifikacijų, kad užtikrintų tvarkomų asmens duomenų apsaugą. Jeigu duomenis tvarko tvarkytojas, organizatoriai turėtų užtikrinti, kad tvarkytojas veiktų tik pagal organizatorių nurodymus ir laikytųsi šiame reglamente nustatytų specifikacijų;

(8) šiuo reglamentu gerbiamos pagrindinės teisės ir atsižvelgiama į Europos Sąjungos pagrindinių teisių chartijoje įtvirtintus principus, visų pirma jos 8 straipsnį, kuriame teigiama, kad kiekvienas turi teisę į savo asmens duomenų apsaugą;

(9) šiame reglamente numatytos priemonės atitinka pagal Reglamento (ES) Nr. 211/2011 20 straipsnį įsteigto komiteto nuomonę,

[1] OL L 65, 2011 3 11, p. 1.

[2] OL L 281, 1995 11 23, p. 31.

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Reglamento (ES) Nr. 211/2011 6 straipsnio 5 dalyje nurodytos specifikacijos yra nustatytos priede.

2 straipsnis

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje.*

Šis reglamentas yra privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2011 m. lapkričio 17 d.

Komisijos vardu
Pirmininkas
José Manuel BARROSO

PRIEDAS

1. REGLAMENTO (ES) Nr. 211/2011 6 STRAIPSNIO 4 DALIES a PUNKTO ĮGYVENDINIMO TECHNINĖS SPECIFIKACIJOS

Kad pasinaudojus sistema pritarimo pareiškimai nebūtų teikiami automatizuotai, pasirašiusiajam asmeniui, prieš jam pateikiant pritarimo pareiškimą, taikoma tinkama patikros procedūra, atitinkanti dabartinę praktiką. Viena iš galimų patikros procedūrų yra patikimas ženklų atpažinimo testas (angl. *captcha*).

2. REGLAMENTO (ES) Nr. 211/2011 6 STRAIPSNIO 4 DALIES b PUNKTO ĮGYVENDINIMO TECHNINĖS SPECIFIKACIJOS

Informacijos apsaugos standartai

2.1. Organizatoriai pateikia dokumentus, kuriais įrodo, kad jie laikosi standarto ISO/IEC 27001 reikalavimų, išskyrus standarto priėmimo reikalavimą. Šiuo tikslu jie turi būti:

a) atlikę išsamų rizikos vertinimą, pagal kurį nustatoma sistemos taikymo sritis, aiškiai nurodomas įvairių informacijos apsaugos pažeidimų poveikis veiklai, išvardijamos informacinei sistemai pavojingos grėsmės ir jos silpnosios vietos, pateikiamas rizikos analizės dokumentas, kuriame taip pat nurodomos atsakomosios priemonės, kaip išvengti šių grėsmių, ir priemonės, kurių bus imtasi iš tiesų kilus grėsmei, taip pat pateikiamas svarbos tvarka sudarytas tobulintinų dalykų sąrašas;

b) parengę ir įgyvendinę rizikos, susijusios su asmens duomenų ir šeimos bei privataus gyvenimo apsauga, mažinimo priemones ir priemones, kurių bus imtasi iš tiesų kilus rizikai;

c) aprašę liekamąją riziką;

d) numatę organizacines priemones, kaip gauti grįžtamosios informacijos apie naujas grėsmes ir saugumo gerinimą.

2.2. Saugumo kontrolės priemonės, kurias pagal 2.1 punkto a papunktyje nurodytą rizikos analizę pasirenka organizatoriai, atitinka šiuos standartus:

1) ISO/IEC 27002 arba

2) Informacijos saugumo forumo Gerosios patirties standartą (angl. *Standard of Good Practice*),

kad būtų išspręsti šie klausimai:

a) rizikos vertinimas (rekomenduojama taikyti standartą ISO/IEC 27005 arba kitokią specialią tinkamą vertinimo metodiką);

b) fizinis ir aplinkos saugumas;

c) žmogiškųjų išteklių saugumas;

d) ryšių ir veiklos valdymas;

e) įprastinės prieigos kontrolės priemonės, kuriomis papildomos šiame įgyvendinimo reglamente nustatytos priemonės;

f) informacinių sistemų įsigijimas, kūrimas ir priežiūra;

g) informacijos saugumo incidentų valdymas;

h) priemonės, kuriomis šalinami ir mažinami informacinių sistemų pažeidimai, dėl kurių tvarkomi asmens duomenys būtų sunaikinti arba atsitiktinai prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami;

i) atitiktis;

j) kompiuterių tinklo saugumas (rekomenduojama taikyti standartą ISO/IEC 27033 arba Gerosios patirties standartą).

Šių standartų taikymas gali būti apribotas tais organizacijos padaliniais, kurie yra susiję su internetine pritarimo pareiškimų rinkimo sistema. Pavyzdžiui, žmogiškųjų išteklių saugumas gali būti užtikrinamas tik tų darbuotojų atžvilgiu, kurie gali fiziškai prieiti arba per tinklą prisijungti prie internetinės pritarimo pareiškimų rinkimo sistemos, o fizinis ir (arba) aplinkos saugumas gali būti apribotas pastatu (-ais), kuriame (-uose) saugoma sistema.

Funkciniai reikalavimai

2.3. Internetinė pritarimo pareiškimų rinkimo sistema yra sudaryta iš internetinio taikomosios programos egzemplioriaus, įdiegto pritarimo pareiškimų rinkimo pagal atskirą piliečių iniciatyvą tikslais.

2.4. Jeigu sistemai tvarkyti reikia įvairių rolių, pagal mažiausio būtino teisių kiekio principą nustatomi įvairūs prieigos kontrolės lygiai.

2.5. Viešai prieinamos funkcijos aiškiai atskiriamos nuo administravimo funkcijų. Jokia prieigos kontrolės priemone neturi būti trukdoma skaityti viešoje sistemos srityje esančios informacijos, įskaitant informaciją apie iniciatyvą ir elektroninę pritarimo pareiškimo formą. Pasirašyti už iniciatyvą turi būti galima tik viešojoje srityje.

2.6. Sistema turi nustatyti atvejus, kai bandoma pakartotinai pateikti pritarimo pareiškimus, ir neleisti pakartotinai jų teikti.

Taikomosios programos lygmens saugumas

2.7. Sistema tinkamai apsaugoma nuo žinomų pažeidimo ir pasinaudojimo pažeidžiamumu būdų. Šiuo tikslu ji, *inter alia*, turi atitikti šiuos reikalavimus:

2.7.1. sistema apsaugota nuo įsilaužimo, pvz., naudojant SQL (angl. *Structured Query Language*), LDAP (angl. *Lightweight Directory Access Protocol*), XPath (angl. *XML Path Language*) užklausas, operacinės sistemos (OS) komandas arba programų argumentus. Todėl būtina bent:

a) tikrinti visą naudotojų įvestį;

b) tikrinti bent serverio logikos priemonėmis;

c) naudojant interpretatorius, aiškiai atskirti nepatikimus duomenis nuo komandų arba užklausų. SQL kreipinių atveju tai reiškia, kad visuose parengtuose sakiniuose ir išsaugotose procedūrose turi būti naudojami susietieji kintamieji ir turi būti vengiama dinaminių užklausų;

2.7.2. sistema apsaugota nuo tarpsvetainininių scenarijų (angl. *Cross-Site Scripting*, XSS). Todėl būtina bent:

a) tikrinti, ar visi naudotojų įvedami duomenys, kurie siunčiami atgal į naršyklę, yra saugūs (taikant įvesties patikrą);

b) tinkamai taikyti kaitos (angl. *escape*) seką visiems naudotojų įvestiems duomenims, prieš juos įtraukiant į galutinį tinklalapį;

c) tinkamu rezultatų kodavimu užtikrinti, kad įvedami duomenys visada būtų tvarkomi kaip tekstas naršyklėje. Aktyvus turinys nenaudojamas;

2.7.3. sistemoje įdiegtos patikimos tapatybės nustatymo ir seanso valdymo priemonės, kuriomis reikalaujama, kad:

a) išsaugomi prisijungimo duomenys visada apsaugomi naudojant maišos arba užšifravimo metodą. Sumažinama rizika, kad kas nors nurodys savo tapatybę pasinaudodamas maišos apėjimo (angl. *pass-the-hash*) metodu;

b) prisijungimo duomenų nebūtų galima atspėti arba perrašyti pasinaudojant nesaugiomis paskyros valdymo funkcijomis (pvz., paskyros kūrimo, slaptažodžio keitimo, slaptažodžio atkūrimo funkcijomis, nesaugiais seanso identifikatoriais);

c) seanso identifikatoriai ir seanso duomenys nebūtų atskleidžiami universaliajame ištekliaus adrese (angl. URL);

d) seanso identifikatoriai nebūtų pažeidžiami seanso fiksavimo atakomis;

e) būtų taikoma seanso identifikatorių skirtojo laiko pabaiga, kuria būtų užtikrintas naudotojų atsijungimas;

f) sėkmingai prisijungus, seanso identifikatoriai nebūtų keičiami;

g) slaptažodžiai, seanso identifikatoriai ir kiti prisijungimo duomenys būtų perduodami tik transporto lygmens saugos (TLS) protokolu;

h) sistemos administravimo dalis būtų apsaugota. Jeigu ji apsaugota naudojant vieno veiksnio tapatybės nustatymo būdą, slaptažodis sudaromas ne mažiau kaip iš 10 ženklų, iš kurių turi būti bent viena raidė, vienas skaitmuo ir vienas specialusis rašmuo. Taip pat gali būti taikomas dviejų veiksnių tapatybės nustatymo būdas. Jeigu taikomas tik vieno veiksnio tapatybės nustatymo būdas, pagal jį turi būti taikomas dviejų pakopų patikros mechanizmas, skirtas internetu prisijungti prie sistemos administravimo dalies, vieną veiksnį papildant kitomis tapatybės nustatymo priemonėmis, pvz., naudojant vienkartinę slaptą frazę arba kodą, perduodamą tekstine žinute, arba asimetriškai užšifruotą atsitiktinę patikros eilutę, kuri turi būti iššifruota naudojant organizatorių arba administratorių asmeninį raktą, kuris sistemai yra nežinomas;

2.7.4. sistemoje nenaudojama nesaugių tiesioginių objektinių sąsajų. Todėl būtina bent:

a) kad tiesioginių nuorodų į ribotos prieigos išteklius atveju taikomoji programa patikrintų, ar naudotojui suteikta teisė naudotis konkrečiu prašomu ištekliumi;

b) tiesioginės nuorodos atvaizdavimą riboti vertėmis, kurios yra leidžiamos tam naudotojui, jeigu nuoroda yra netiesioginė;

2.7.5. sistema apsaugota nuo tarpsvetainių užklausų klastojimo;

2.7.6. nustatoma tinkama saugos sąranka, laikantis bent šių reikalavimų:

a) atnaujinamos visos programinės įrangos sudedamosios dalys, įskaitant OS, svetainės ir (arba) taikomosios programos serverio programinę įrangą, duomenų bazės valdymo sistemą, taikomąsias programas ir visas kodų bibliotekas;

b) operacinėje sistemoje ir svetainės ir (arba) taikomosios programos serveryje visos nebūtinos tarnybos išjungiamos, pašalinamos arba apskritai neįdiegiamos;

c) pakeičiami arba panaikinami numatytieji paskyrų slaptažodžiai;

d) klaidų apdorojimas nustatomas taip, kad būtų išvengta dėklo trasavimo ir kitų pernelyg informatyvių pranešimų apie klaidas atskleidimo;

e) programavimo aplinkos ir bibliotekų saugumo nuostatos nustatomos atsižvelgiant į geriausiąją patirtį, pvz., OWASP gaires;

2.7.7. sistema suteikia galimybę užšifruoti duomenis tokiu būdu:

a) saugomi arba valstybių narių kompetentingoms institucijoms pagal Reglamento (ES) Nr. 211/2011 8 straipsnio 1 dalį elektronine forma teikiami asmens duomenys užšifruojami, raktai valdomi ir atsarginės jų kopijos saugomos atskirai;

b) laikantis tarptautinių standartų naudojami patikimi standartiniai algoritmai ir patikimi raktai. Įdiegta raktų valdymo sistema;

c) slaptažodžių maiša atliekama taikant patikimą standartinį algoritmą, šifruojant įterpiamas atsitiktinis skaičius (angl. *salt*);

d) visi raktai ir slaptažodžiai saugomi nuo nesankcionuotos prieigos;

2.7.8. sistema riboja URL prieigą pagal naudotojo prieigos lygmenis ir leidimus. Šiuo tikslu taikomi bent šie reikalavimai:

a) jeigu atveriant tinklalapį tapatybei patvirtinti ir teisėms patikrinti naudojami išoriniai saugumo mechanizmai, jie turi būti tinkamai konfigūruoti pagal kiekvieną tinklalapį;

b) jeigu taikoma kodo lygmens apsauga, ji turi būti taikoma kiekvienam prašomam tinklalapiui;

2.7.9. sistemoje naudojama pakankama TLS. Šiuo tikslu turi būti įdiegtos visos šios priemonės (arba ne mažiau kaip lygiaverčio patikimumo priemonės):

a) pagal sistemą reikalaujama, kad slaptiems ištekliams pasiekti būtų naudojama naujausia saugaus hipertekstų persiuntimo protokolo (HTTPS) versija ir teisėti, nepasibaigusio galiojimo, neatšaukti ir visoms svetainės sritims taikomi sertifikatai;

b) sistema visus su slaptąja informacija siejamus slapukus pažymi gairele „saugus“;

c) serveryje nustatoma tokia TLS teikėjo konfigūracija, kad būtų galima taikyti tik geriausiąją patirtį atitinkančius užšifravimo algoritmus, naudotojai informuojami, kad jie savo naršyklėje turi įjungti TLS palaikymą;

2.7.10. sistema apsaugota nuo netinkamo peradresavimo ir persiuntimo.

Duomenų bazės saugumas ir duomenų vientisumas

2.8. Jeigu įvairioms piliečių iniciatyvoms naudojamos internetinės pritarimo pareiškimų rinkimo sistemos dalijasi aparatinės įrangos ir operacinės sistemos ištekliais, jos nesidalija jokiais duomenimis, įskaitant prieigos ir (arba) užšifravimo duomenis. Be to, į tai atsižvelgiama atliekant rizikos vertinimą ir įgyvendinant atsakomąsias priemones.

2.9. Sumažinama rizika, kad kas nors prisijungs prie duomenų bazės pasinaudojęs maišos apėjimo metodu.

2.10. Prieiga prie pasirašiusiųjų asmenų pateiktų duomenų suteikiama tik duomenų bazės administratoriui ir (arba) organizatoriui.

2.11. Administravimo tikslais naudojami prisijungimo duomenys, iš pasirašiusiųjų asmenų surinkti asmens duomenys ir jų atsarginės kopijos saugomos naudojant patikimus užšifravimo algoritmus, laikantis 2.7.7 skirsnio b punkto. Tačiau valstybė narė, kuriai bus įskaičiuotas pritarimo pareiškimas, pritarimo pareiškimo pateikimo data ir kalba, kuria pasirašiusysis asmuo užpildė pritarimo pareiškimo formą, sistemoje gali būti saugomos neužšifruotos.

2.12. Pasirašiusiesiems asmenims suteikiama prieiga tik prie tų duomenų, kurie seanso metu pateikiami pildant pritarimo pareiškimo formą. Pateikus pritarimo pareiškimą, pirmiau minėtas seansas nutraukiamas, ir prieiga prie pateiktų duomenų nebesuteikiama.

2.13. Pasirašiusiųjų asmenų asmens duomenys, įskaitant atsarginę kopiją, sistemoje saugomi tik užšifruoti. Duomenų peržiūrėjimo arba nacionalinių valdžios institucijų pagal Reglamento (ES) Nr. 211/2011 8 straipsnį atliekamo sertifikavimo tikslais organizatoriai gali eksportuoti užšifruotus duomenis pagal 2.7.7 skirsnio a punktą.

2.14. Pritarimo pareiškime pateikti duomenys neskaidomi. Tai reiškia, kad naudotojui į pritarimo pareiškimą įrašius visus reikiamus duomenis ir jam patvirtinus savo sprendimą paremti iniciatyvą, sistema perduoda visus formos duomenis į duomenų bazę arba, jeigu įvyksta klaida, neišsaugo jokių duomenų. Sistema praneša naudotojui apie tai, ar jo užklausa buvo sėkminga, ar ne.

2.15. Naudojama duomenų bazės valdymo sistema turi būti atnaujinama ir nuolat taisoma atsižvelgiant į nustatytus naujus pasinaudojimo pažeidžiamumu būdus.

2.16. Saugomi visi sistemos veikimo žurnalai. Sistema užtikrina, kad audito žurnalai, kuriuose užregistruotos išimtinės situacijos ir kiti toliau nurodyti saugumo atžvilgiu svarbūs įvykiai, būtų rengiami ir saugomi, kol duomenys nesunaikinami pagal Reglamento (ES) Nr. 211/2011 12 straipsnio 3 arba 5 dalis. Žurnalai yra tinkamai apsaugoti, pvz., jie saugojami užšifruotose laikmenose. Organizatoriai ir (arba) administratoriai periodiškai žurnaluose tikrina, ar nebuvo atlikta įtartinų veiksmų. Žurnaluose pateikiami bent šie duomenys:

a) organizatorių ir (arba) administratorių prisijungimo ir atsijungimo datos ir laikas;

b) padarytos atsarginės kopijos;

c) visi duomenų bazės administratoriaus padaryti pakeitimai ir atnaujinimo operacijos.

Infrastruktūros saugumas. Fizinė vieta, tinklo infrastruktūra ir serverio aplinka

2.17. *Fizinis saugumas:*

kad ir kokio tipo priegloba būtų naudojama, kompiuteris, kuriame įdiegta taikomoji programa, turi būti tinkamai apsaugotas šiomis priemonėmis:

a) patekimo į kompiuterio buvimo vietą kontrolė ir audito žurnalas;

b) fizinė atsarginės duomenų kopijos apsauga nuo vagystės arba netyčinio palikimo netinkamoje vietoje;

c) serverio, kuriame įdiegiama taikomoji programa, įrengimas apsaugotoje spintoje.

2.18. *Tinklo saugumas:*

2.18.1. sistema įdiegiama prie interneto prijungtame serveryje, įrengtame demilitarizuotoje zonoje (DMZ) ir apsaugotame ugniasiene;

2.18.2. kuo skubiau įdiegiami paskelbti svarbūs ugniasienės produkto naujiniai ir pataisos;

2.18.3. visi į serverį gaunamų ir iš jo siunčiamų duomenų srautai (skirti internetinei pritarimo pareiškimų rinkimo sistemai) tikrinami pagal ugniasienės taisykles ir registruojami žurnale. Pagal ugniasienės taisykles blokuojami visi duomenų srautai, kurie nėra būtini saugiam sistemos naudojimui ir administravimui;

2.18.4. internetinės pritarimo pareiškimų rinkimo sistemos priegloba turi būti tinkamai apsaugotame darbinio tinklo segmente, atskirtame nuo segmentų, naudojamų nedarbinių sistemų, pvz., programavimo ir bandymo aplinkos, prieglobai;

2.18.5. turi būti taikomos vietinio tinklo (LAN) saugumo priemonės, pvz.:

a) 2 lygmens (L2) prieigos sąrašas / prievadų perjungimo apsauga;

b) nenaudojami prievadai išjungiami;

c) DMZ yra skirtiniame virtualiajame vietiniame tinkle (VLAN) arba vietiniame tinkle (LAN);

d) nereikalinguose prievaduose neleidžiama naudoti L2 sutelkimo.

2.19. *OS ir svetainės ir (arba) taikomosios programos serverio saugumas:*

2.19.1. nustatoma tinkama saugumo konfigūracija, įskaitant 2.7.6 punkte nurodytus elementus;

2.19.2. taikomosios programos veikia pagal mažiausią joms veikti būtiną teisių rinkinį;

2.19.3. naudojamas trumpas (ne ilgesnis kaip 15 minučių) administratoriaus prieigos prie internetinės pritarimo pareiškimų rinkimo sistemos valdymo sąsajos seanso skirtasis laikas;

2.19.4. kuo skubiau įdiegiami paskelbti svarbūs OS, taikomosios programos vykdymo, serveryje veikiančių taikomųjų programų arba kovai su kenkimo programine įranga skirtų priemonių naujiniai ir pataisos;

2.19.5. sumažinama rizika, kad kas nors prisijungs prie sistemos pasinaudojęs maišos apėjimo metodu.

2.20. *Organizatoriaus kliento įrangos saugumas.*

Siekdami užtikrinti perdavimo linijos apsaugą organizatoriai imasi būtinų savo kliento programos ir (arba) įrenginio, kurią (-į) jie naudoja internetinei pritarimo pareiškimų rinkimo sistemai valdyti ir prie jos prisijungti, apsaugos priemonių, pvz.:

2.20.1. naudotojai paleidžia ne priežiūros tikslais naudojamas, pvz., biuro darbo automatizavimo, programas naudodami mažiausią joms veikti būtiną teisių rinkinį;

2.20.2. kuo skubiau įdiegiami paskelbti svarbūs OS, įdiegtų taikomųjų programų arba kovai su kenkimo programine įranga skirtų priemonių naujiniai ir pataisos.

3. REGLAMENTO (ES) NR. 211/2011 6 STRAIPSNIO 4 DALIES c PUNKTO ĮGYVENDINIMO TECHNINĖS SPECIFIKACIJOS

3.1. Sistema suteikia galimybę kiekvienai valstybei narei parengti nurodytos iniciatyvos ataskaitą ir išrinkti pasirašiusiųjų asmenų asmens duomenis, kuriuos turi patikrinti valstybės narės kompetentinga institucija.

3.2. Pasirašiusiųjų asmenų pritarimo pareiškimai gali būti eksportuojami Reglamento (ES) Nr. 211/2011 III priede nustatytu formatu. Be to, sistemoje gali būti numatyta galimybė eksportuoti pritarimo pareiškimus sąveikiuoju, pvz., XML, formatu.

3.3. Eksportuotieji pritarimo pareiškimai pažymimi kaip *riboto platinimo* atitinkamoje valstybėje narėje ir kaip *asmens duomenys*.

3.4. Taikant tinkamą perdavimo linijos šifravimą, elektroninis eksportuotų duomenų perdavimas valstybėms narėms apsaugomas nuo slapto nuskaitymo.