REGLAMENTAI

KOMISIJOS REGLAMENTAS (ES) Nr. 611/2013

2013 m. birželio 24 d.

dėl priemonių, kurios pagal Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl privatumo ir elektroninių ryšių taikomos pranešimams apie asmens duomenų saugumo pažeidimus

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvą Nr. 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) ([1]), ypač į jos 4 straipsnio 5 dalį,

pasikonsultavusi su Europos tinklų ir informacijos apsaugos agentūra (ENISA),

pasikonsultavusi su Asmenų apsaugos tvarkant asmens duomenis darbo grupe, įsteigta pagal 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ([2]) 29 straipsnį (29 straipsnio darbo grupe),

pasikonsultavusi su Europos duomenų apsaugos priežiūros pareigūnu (EDAPP),

kadangi:

(1) Direktyvoje 2002/58/EB numatytas valstybių narių nuostatų, užtikrinančių vienodo lygio pagrindinių teisių ir laisvių, ypač teisės į privatumą ir konfidencialumą, apsaugą, susijusių su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, ir užtikrinančių laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų judėjimą Sąjungoje, suderinimas;

(2) pagal Direktyvos 2002/58/EB 4 straipsnį viešai prieinamų elektroninių ryšių paslaugų teikėjai įpareigoti informuoti kompetentingas nacionalines institucijas (tam tikrais atvejais – ir susijusius abonentus bei fizinius asmenis) apie asmens duomenų saugumo pažeidimus. Kaip apibrėžta Direktyvos 2002/58/EB 2 straipsnio i punkte, asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio atsitiktinai arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami asmens duomenys arba atsiranda galimybė naudotis tais duomenimis, kai jie buvo perduodami, saugomi arba kitaip tvarkomi teikiant viešąją elektroninių ryšių paslaugą Sąjungoje;

(3) siekiant užtikrinti darnų Direktyvos 2002/58/EB 4 straipsnio 2, 3 ir 4 dalyse nurodytų priemonių įgyvendinimą, jos 4 straipsnio 5 dalimi Komisijai suteikti įgaliojimai priimti technines įgyvendinimo priemones, susijusias su tame straipsnyje nurodytiems informavimo ir pranešimo reikalavimams taikomomis aplinkybėmis, forma ir tvarka;

(4) dėl skirtingų nacionalinių šios srities reikalavimų taikymo teikėjai, vykdantys veiklą tarpvalstybiniu mastu, gali patirti teisinį netikrumą, susidurti su sudėtingesnėmis varžančiomis procedūromis ir turėti didelių administracinių sąnaudų. Todėl Komisija mano, kad būtina priimti tokias technines įgyvendinimo priemones;

(5) šio reglamento taikymo sritis apima tik pranešimą apie asmens duomenų saugumo pažeidimus, todėl jame nenumatytos techninės įgyvendinimo priemonės, susijusios su Direktyvos 2002/58/EB 4 straipsnio 2 dalimi dėl abonentų informavimo iškilus tam tikrai tinklo saugumo pažeidimo rizikai;

(6) remiantis Direktyvos 2002/58/EB 4 straipsnio 3 dalies pirma pastraipa, paslaugų teikėjai kompetentingai nacionalinei institucijai turi pranešti apie visus asmens duomenų saugumo pažeidimus. Todėl teikėjui neturėtų būti leista savo nuožiūra spręsti, ar pranešti apie asmens duomenų saugumo pažeidimą kompetentingai nacionalinei institucijai. Tačiau atitinkamai kompetentingai nacionalinei institucijai tai neturėtų trukdyti pagal galiojančius įstatymus tam tikrus pažeidimus savo nuožiūra nagrinėti pirmumo tvarka ir prireikus imtis veiksmų, kad būtų išvengta netikslumų, susijusių su asmens duomenų pažeidimų, apie kuriuos pranešama, skaičiumi;

(7) reikėtų nustatyti pranešimo kompetentingai nacionalinei institucijai apie asmens duomenų saugumo pažeidimus sistemą, kurioje būtų numatyta, kad tam tikromis sąlygomis tam tikrą ribotą laikotarpį įgyvendinami įvairūs etapai. Taikant šią sistemą turėtų būti užtikrinama, kad kompetentinga nacionalinė institucija būtų informuojama kuo anksčiau, tačiau paslaugų teikėjui nebūtų trukdoma nagrinėti pažeidimą ir imtis reikiamų priemonių apriboti pažeidimo mastą ir pašalinti jo pasekmes;

([1]) OL L 201, 2002 7 31, p. 37.
([2]) OL L 281, 1995 11 23, p. 31.

(8) vien įtarimo, kad įvyko asmens duomenų saugumo pažeidimas, arba vien saugumo incidento nustatymo, kai neturima pakankamai informacijos, nors teikėjas dėjo visas pastangas jos gauti, nepakanka, kad pagal šį reglamentą būtų laikoma, jog nustatytas asmens duomenų saugumo pažeidimas. Šiuo atžvilgiu turėtų būti ypač svarbu turėti I priede nurodytą informaciją;

(9) taikant šį reglamentą tarpvalstybinio pobūdžio asmens duomenų saugumo pažeidimus susijusios kompetentingos nacionalinės institucijos nagrinėja bendradarbiaudamos;

(10) šiame reglamente nenumatyta jokia papildoma pagal Direktyvos 2002/58/EB 4 straipsnį teikėjų tvarkomo asmens duomenų saugumo pažeidimų registro specifikacija. Tačiau teikėjai gali nustatyti tokio registro formą vadovaudamiesi šiuo reglamentu;

(11) visos kompetentingos nacionalinės institucijos turėtų teikti saugias elektronines priemones, kuriomis naudodamiesi teikėjai galėtų atitinkamomis kalbomis pateikti I priede nurodytą bendros formos (pvz., grindžiamos XML standartu) informaciją, kad visoje Sąjungoje būtų laikomasi panašios pranešimo tvarkos, kad ir kur būtų įsisteigęs teikėjas ar būtų įvykdytas asmens duomenų saugumo pažeidimas. Tuo atžvilgiu Komisija turėtų palengvinti saugių elektroninių priemonių įgyvendinimą ir tuo tikslu prireikus rengti posėdžius su kompetentingomis nacionalinėmis institucijomis;

(12) vertinant, ar asmens duomenų saugumo pažeidimas gali turėti neigiamą poveikį asmens duomenims arba abonento ar fizinio asmens privatumui, visų pirma turėtų būti atsižvelgta į atitinkamų asmens duomenų pobūdį ir turinį, ypač kai duomenys yra susiję su finansine informacija, pavyzdžiui, kai tai kredito kortelių duomenys ir informacija apie banko sąskaitą; ypatingų kategorijų duomenys, nurodyti Direktyvos 95/46/EB 8 straipsnio 1 dalyje; taip pat tam tikri duomenys, konkrečiai susiję su telefonijos ar interneto paslaugų teikimu, t. y. e. pašto duomenys, vietos nustatymo duomenys, interneto įeičių dienynų failai, interneto naršymo istorija ir detalūs iškvietų sąrašai;

(13) išskirtinėmis aplinkybėmis teikėjui turėtų būti leidžiama pranešimą abonentui arba fiziniam asmeniui atidėti, jei dėl pranešimo galbūt būtų apsunkintas tinkamas asmens duomenų saugumo pažeidimo tyrimas. Todėl prie išskirtinių aplinkybių gali būti priskiriamas baudžiamųjų veikų tyrimas, taip pat kiti asmens duomenų saugumo pažeidimai, kurie neprilygsta sunkiam nusikaltimui, tačiau kurių atveju gali būti tikslinga atidėti pranešimą. Bet kuriuo atveju kompetentinga nacionalinė institucija turėtų įvertinti kiekvieną konkretų atvejį ir, atsižvelgdama į aplinkybes, nuspręsti, ar sutikti su pranešimo atidėjimu, ar reikalauti pranešimą pateikti nedelsiant;

(14) nors teikėjai dėl tiesioginių sutartinių santykių su savo abonentais turėtų turėti jų kontaktinius duomenis, tokios informacijos apie kitus fizinius asmenis, kuriems dėl asmens duomenų saugumo pažeidimo padarytas neigiamas poveikis, jie gali neturėti. Tokiu atveju, siekiant apie tai pranešti tiems fiziniams asmenims, teikėjui turėtų būti leidžiama iš pradžių įdėti atitinkamą skelbimą pagrindinėse nacionalinėse arba regioninėse žiniasklaidos priemonėse, pavyzdžiui, laikraščiuose, o po to kuo greičiau pateikti individualų pranešimą, kaip numatyta šiame reglamente. Todėl iš esmės teikėjas ne įpareigojamas pranešti per žiniasklaidos priemones, o tik įgaliojamas tai padaryti savo nuožiūra, kol nustatinėjami visi fiziniai asmenys, kuriems padarytas poveikis;

(15) informacija apie pažeidimą turėtų būti susijusi tik su tuo pažeidimu ir nesiejama su jokia kita informacija. Pavyzdžiui, informacijos apie asmens duomenų saugumo pažeidimą pateikimas įprastoje sąskaitoje faktūroje neturėtų būti laikomas tinkama priemone pranešti apie asmens duomenų saugumo pažeidimą;

(16) šiuo reglamentu nenustatoma konkrečių technologinių apsaugos priemonių, kuriomis būtų galima pagrįsti nukrypimą nuo įpareigojimo pranešti abonentams arba fiziniams asmenims apie asmens duomenų saugumo pažeidimus, nes technologijoms tobulėjant tokios priemonės ilgainiui gali keistis. Tačiau Komisija pagal galiojančią tvarką turėtų turėti galimybę skelbti tokių konkrečių technologinės apsaugos priemonių orientacinį sąrašą;

(17) neturėtų būti laikoma, kad šifravimo arba maišos pakanka, kad teikėjai galėtų plačiau pareikšti, jog yra įvykdę bendrąjį saugumo įpareigojimą pagal Direktyvos 95/46/EB 17 straipsnį. Šiuo atžvilgiu teikėjai taip pat turėtų įgyvendinti tinkamas organizacines ir technines priemones, kad išvengtų asmens duomenų saugumo pažeidimų, juos aptiktų ir užkirstų jiems kelią. Teikėjai turėtų įvertinti riziką, kuri galbūt lieka įgyvendinus kontrolės priemones, kad suprastų, kur gali įvykti asmens duomenų saugumo pažeidimų;

(18) kai teikėjas paslaugą iš dalies teikia naudodamasis kito teikėjo paslaugomis, pavyzdžiui, susijusiomis su

sąskaitų išrašymu ar valdymu, pastarasis teikėjas, kuris su galutiniu naudotoju nėra tiesiogiai susietas sutartiniais santykiais, asmens duomenų saugumo pažeidimo atveju neturėtų būti įpareigojamas pateikti pranešimus. Jis tik turėtų įspėti ir informuoti teikėją, su kuriuo yra tiesiogiai susietas sutartiniais santykiais. Tai turėtų būti taikoma ir teikiant didmenines elektroninių ryšių paslaugas, kai didmeninės paslaugos teikėjas su galutiniu vartotoju paprastai nėra tiesiogiai susietas sutartiniais santykiais;

(19) Direktyva Nr. 95/46/EB nustatyta bendroji asmens duomenų apsaugos Europos Sąjungoje sistema. Komisija pateikė Europos Parlamento ir Tarybos reglamento, kuriuo būtų pakeista Direktyva 95/46/EB, (Duomenų apsaugos reglamento) pasiūlymą. Pasiūlytu Duomenų apsaugos reglamentu visi duomenų valdytojai, remiantis Direktyvos 2002/58/EB 4 straipsnio 3 dalimi, būtų įpareigojami pranešti apie asmens duomenų saugumo pažeidimus. Šis Komisijos reglamentas visiškai atitinka minėtą pasiūlytą priemonę;

(20) pasiūlytu Duomenų apsaugos reglamentu padaromas ir tam tikras ribotas skaičius techninių Direktyvos 2002/58/EB pakeitimų, kad būtų atsižvelgta į tai, kad Direktyva 95/46/EB pakeičiama reglamentu. Komisija apsvarstys, kokių svarbių teisinių padarinių naujasis reglamentas turės Direktyvai 2002/58/EB;

(21) šio reglamento taikymą reikėtų persvarstyti praėjus trejiems metams po jo įsigaliojimo, o jo turinys turėtų būti persvarstomas atsižvelgiant į tuo metu galiojančią teisinę sistemą, įskaitant pasiūlytą Duomenų apsaugos reglamentą. Šio reglamento persvarstymas turėtų būti siejamas, jei įmanoma, su galimu būsimu Direktyvos 2002/58/EB persvarstymu;

(22) šio reglamento taikymas galėtų būti vertinamas remiantis, *inter alia*, visais kompetentingų nacionalinių institucijų tvarkomais asmens duomenų saugumo pažeidimų, apie kuriuos joms pranešama, statistiniais duomenimis. Tai, pavyzdžiui, gali būti informacija apie asmens duomenų saugumo pažeidimų, apie kuriuos pranešta kompetentingai nacionalinei institucijai, skaičių, apie asmens duomenų saugumo pažeidimų, apie kuriuos pranešta abonentams arba fiziniams asmenims, skaičių, apie tai, kiek laiko užtruko išspręsti asmens duomenų saugumo pažeidimą ir ar imtasi technologinių apsaugos priemonių. Teikiant šią statistinę informaciją Komisijai ir valstybėms narėms turėtų būti pateikiami nuoseklūs ir palyginami statistiniai duomenys, neatskleidžiant nei pranešančiojo teikėjo, nei susijusių abonentų ar fizinių asmenų tapatybės. Be to, Komisija šiuo tikslu gali reguliariai rengti susitikimus su kompetentingomis nacionalinėmis institucijomis ir kitomis suinteresuotosiomis šalimis;

(23) šiame reglamente numatytos priemonės atitinka Ryšių komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Taikymo sritis

Šis reglamentas taikomas viešai prieinamų elektroninių ryšių paslaugų teikėjo (toliau – teikėjas) pranešimui apie asmens duomenų saugumo pažeidimus.

2 straipsnis

Pranešimas kompetentingai nacionalinei institucijai

1. Apie visus asmens duomenų saugumo pažeidimus teikėjas praneša kompetentingai nacionalinei institucijai.

2. Kai įmanoma, apie asmens duomenų saugumo pažeidimą teikėjas kompetentingai nacionalinei institucijai praneša per 24 valandas nuo asmens duomenų saugumo pažeidimo nustatymo.

Teikėjas pranešime kompetentingai nacionalinei institucijai pateikia I priede nustatytą informaciją.

Laikoma, kad asmens duomenų saugumo pažeidimas padarytas, kai teikėjas sužino apie saugumo incidentą, dėl kurio buvo pažeistas asmens duomenų saugumas, kad pagal šį reglamentą galėtų pateikti tinkamą pranešimą.

3. Kai visos I priede nurodytos informacijos neturima ir būtina atlikti išsamesnį asmens duomenų saugumo pažeidimo tyrimą, teikėjui leidžiama per 24 valandas nuo asmens duomenų saugumo pažeidimo nustatymo kompetentingai nacionalinei institucijai pateikti pirminį pranešimą. Tame pirminiame pranešime kompetentingai nacionalinei institucijai pateikiama I priedo 1 skirsnyje nurodyta informacija. Teikėjas kuo greičiau ir ne vėliau kaip per tris dienas nuo pradinio pranešimo pateikimo kompetentingai nacionalinei institucijai pateikia antrą pranešimą. Antrajame pranešime pateikiama I priedo 2 skirsnyje nurodyta informacija ir prireikus atnaujinama anksčiau pateikta informacija.

Jeigu teikėjas, nepaisant jo atlikto tyrimo, negali pateikti visos informacijos per tris dienas nuo pirminio pranešimo, jis kompetentingai nacionalinei institucijai praneša visą tuo metu turimą informaciją ir pagrįstai nurodo, kodėl bus vėluojama pateikti likusią informaciją. Teikėjas kompetentingai nacionalinei institucijai kuo greičiau pateikia likusią informaciją ir prireikus atnaujina anksčiau pateiktą informaciją.

4. Kompetentinga nacionalinė institucija visiems toje valstybėje narėje įsisteigusiems teikėjams pateikia saugias elektronines pranešimo apie asmens duomenų saugumo pažeidimus priemones ir informaciją apie tų priemonių prieigos ir naudojimo tvarką. Kad palengvintų šios nuostatos taikymą, prireikus Komisija rengia susitikimus su kompetentingomis nacionalinėmis institucijomis.

5. Kai asmens duomenų saugumo pažeidimas turi poveikį kitų valstybių narių abonentams ar fiziniams asmenims, kompetentinga nacionalinė institucija, kuriai pranešta apie asmens duomenų saugumo pažeidimą, informuoja kitas atitinkamas nacionalines institucijas.

Kad palengvintų šios nuostatos taikymą, Komisija sukuria ir tvarko kompetentingų nacionalinių institucijų ir atitinkamų informacinių punktų sąrašą.

3 straipsnis

Pranešimas abonentui arba fiziniam asmeniui

1. Kai tikėtina, kad asmens duomenų saugumo pažeidimas gali turėti neigiamą poveikį asmens duomenims arba abonento ar fizinio asmens privatumui, teikėjas ne tik pateikia 2 straipsnyje nurodytą pranešimą, bet ir apie pažeidimą praneša susijusiam abonentui arba fiziniam asmeniui.

2. Ar asmens duomenų saugumo pažeidimas gali turėti neigiamą poveikį asmens duomenims arba abonento ar fizinio asmens privatumui, vertinama atsižvelgiant, visų pirma, į tokias aplinkybes:

a) atitinkamų asmens duomenų pobūdį ir turinį, ypač kai tai su finansine informacija susiję duomenys, Direktyvos 95/46/EB 8 straipsnio 1 dalyje nurodyti ypatingų kategorijų duomenys, taip pat vietos nustatymo duomenys, interneto įeičių dienynų failai, interneto naršymo istorija, e. pašto duomenys ir detalūs iškvietų sąrašai;

b) tikėtinas asmens duomenų saugumo pažeidimo pasekmes atitinkamam abonentui arba fiziniam asmeniui, visų pirma jei dėl pažeidimo galima tapatybės vagystė ar tapatybės klastojimas, fizinė žala, psichologinė įtampa, pažeminimas ar žala reputacijai, ir

c) asmens duomenų saugumo pažeidimo aplinkybes, ypač kai duomenys buvo pavogti arba kai teikėjas žino, kad duomenimis neteisėtai disponuoja trečioji šalis.

3. Nustačius asmens duomenų saugumo pažeidimą, abonentui arba fiziniam asmeniui turėtų būti pranešama nedelsiant, kaip nustatyta 2 straipsnio 2 dalies trečioje pastraipoje. Šis pranešimas teikiamas nepriklausomai nuo 2 straipsnyje nurodyto kompetentingai nacionalinei institucijai teikiamo pranešimo apie asmens duomenų saugumo pažeidimą.

4. Teikėjas pranešime abonentui arba fiziniam asmeniui pateikia II priede nustatytą informaciją. Pranešimas abonentui arba fiziniam asmeniui pateikiamas aiškiai ir lengvai suprantama kalba. Teikėjas nesinaudoja pranešimu siekdamas skatinti užsisakyti naujas ar papildomas paslaugas ar jas reklamuoti.

5. Kai dėl pranešimo abonentui arba fiziniam asmeniui gali būti apsunkintas tinkamas asmens duomenų saugumo pažeidimo tyrimas, teikėjui, gavusiam kompetentingos nacionalinės institucijos sutikimą, išskirtinėmis aplinkybėmis leidžiama pranešimą abonentui arba fiziniam asmeniui atidėti tol, kol kompetentinga nacionalinė institucija nuspręs, kad jau galima pagal šį straipsnį pranešti apie asmens duomenų saugumo pažeidimą.

6. Teikėjas abonentui arba fiziniam asmeniui praneša apie asmens duomenų saugumo pažeidimą naudodamasis ryšio priemonėmis, kuriomis naudojantis užtikrinama, kad informacija būtų gaunama greitai, ir kurios yra tinkamai apsaugotos atsižvelgiant į naujausius technikos laimėjimus. Informacija apie pažeidimą yra skiriama tik tam pažeidimui ir nesiejama su jokia kita informacija.

7. Jeigu tiesiogiai su galutiniu vartotoju sutartiniais santykiais susietas teikėjas, nepaisant to, kad ėmėsi reikiamų pastangų, per 3 dalyje nurodytą laikotarpį negali nustatyti visų fizinių asmenų, kuriems asmens duomenų saugumo pažeidimas galėjo turėti neigiamą poveikį, jis per tą laikotarpį gali informuoti tuos fizinius asmenis skelbimu pagrindinėse nacionalinėse arba regioninėse žiniasklaidos priemonėse atitinkamose valstybėse narėse. Tuose skelbimuose pateikiama (jei reikia – glausta forma) II priede nurodyta informacija. Tokiu atveju teikėjas ir toliau deda visas pagrįstas pastangas, kad nustatytų tuos fizinius asmenis ir kuo greičiau praneštų jiems II priede nurodytą informaciją.

4 straipsnis

Technologinės apsaugos priemonės

1. Nukrypstant nuo 3 straipsnio 1 dalies, apie asmens duomenų saugumo pažeidimą pranešti susijusiam abonentui arba fiziniam asmeniui nereikalaujama, jeigu teikėjas kompetentingai institucijai tinkamai įrodė, kad jis įgyvendino tinkamas technologines apsaugos priemones ir kad tos priemonės buvo taikomos duomenims, kurių saugumas buvo pažeistas. Tokiomis technologinėmis apsaugos priemonėmis užtikrinama, kad asmeniui, neturinčiam leidimo su duomenimis susipažinti, jie būtų neįskaitomi.

2. Duomenys laikomi neįskaitomais, jeigu:

a) jie buvo saugiai užšifruoti pagal standartizuotą algoritmą, duomenų iššifravimo rakto saugumas nebuvo pažeistas per jokį saugumo pažeidimą ir duomenų iššifravimo raktas buvo sugeneruotas taip, kad esamomis technologinėmis priemonėmis jo negalėtų nustatyti joks asmuo, neturintis leidimo naudotis raktu; arba

b) jie buvo pakeisti maišos rezultatu, apskaičiuotu naudojant standartizuotą raktinės maišos funkciją, duomenų maišos rakto saugumas nebuvo pažeistas per jokį saugumo pažeidimą, o duomenų maišos raktas buvo sugeneruotas taip, kad esamomis technologinėmis priemonėmis jo negalėtų nustatyti joks asmuo, neturintis leidimo naudotis raktu.

3. Pasikonsultavusi per 29 straipsnio darbo grupę su kompetentingomis nacionalinėmis institucijomis, Europos tinklų ir informacijos apsaugos agentūra ir Europos duomenų apsaugos priežiūros pareigūnu, Komisija pagal galiojančią tvarką gali paskelbti tinkamų šio straipsnio 1 dalyje nurodytų technologinių apsaugos priemonių orientacinį sąrašą.

5 straipsnis

Naudojimasis kito teikėjo paslaugomis

Kai teikėjas elektroninių ryšių paslaugą iš dalies teikia naudodamasis kito teikėjo, kuris su abonentais nėra tiesiogiai susietas sutartiniais santykiais, paslaugomis, pastarasis teikėjas asmens duomenų saugumo pažeidimo atveju nedelsdamas informuoja teikėją, su kuriuo yra sudaręs paslaugos teikimo sutartį.

6 straipsnis

Persvarstymas ir ataskaitų teikimas

Per trejus metus nuo šio reglamento įsigaliojimo Komisija parengia šio reglamento taikymo, veiksmingumo ir poveikio teikėjams, abonentams ir fiziniams asmenims ataskaitą. Remdamasi ta ataskaita Komisija persvarsto šį reglamentą.

7 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja 2013 m. rugpjūčio 25 d.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2013 m. birželio 24 d.

Komisijos vardu
Pirmininkas
José Manuel BARROSO

I PRIEDAS

Pranešimo kompetentingai nacionalinei institucijai turinys

1 skirsnis

Teikėjo identifikavimas

1. Teikėjo pavadinimas

2. Duomenų apsaugos pareigūno tapatybė ir kontaktiniai duomenys arba kitas informacinis punktas, kur galima gauti išsamesnės informacijos

3. Ar tai pirmas, ar antras pranešimas

Pirminė informacija apie asmens duomenų saugumo pažeidimą (jei taikoma, papildoma vėlesniuose pranešimuose)

4. Incidento data ir laikas (jei žinomi; prireikus gali būti nurodoma numanoma data ir laikas) ir incidento nustatymo data ir laikas

5. Asmens duomenų saugumo pažeidimo aplinkybės (pvz., praradimas, vagystė, nukopijavimas)

6. Susijusių asmens duomenų pobūdis ir turinys

7. Paveiktiems asmens duomenims teikėjo taikytos (arba numatytos taikyti) techninės ir organizacinės priemonės

8. Naudojimasis kitų teikėjų paslaugomis (kai taikoma)

2 skirsnis

Išsamesnė informacija apie asmens duomenų saugumo pažeidimą

9. Incidento, per kurį buvo pažeistas asmens duomenų saugumas, santrauka (įskaitant pažeidimo fizinę vietą ir susijusias laikmenas)

10. Paveiktų abonentų arba fizinių asmenų skaičius

11. Galimos pasekmės ir galimas neigiamas poveikis abonentams arba fiziniams asmenims

12. Techninės ir organizacinės priemonės, kurių ėmėsi teikėjas, kad sumažintų galimą neigiamą poveikį

Galimas papildomas pranešimas abonentams arba fiziniams asmenims

13. Pranešimo turinys

14. Naudotos pranešimo perdavimo priemonės

15. Abonentų arba fizinių asmenų, kuriems pranešta, skaičius

Galimi tarpvalstybiniai klausimai

16. Asmens duomenų saugumo pažeidimas susijęs su abonentais arba fiziniais asmenimis kitose valstybėse narėse

17. Kitų kompetentingų nacionalinių institucijų informavimas

II PRIEDAS

Pranešimo abonentui arba fiziniam asmeniui turinys

1. Teikėjo pavadinimas

2. Duomenų apsaugos pareigūno tapatybė ir kontaktiniai duomenys arba kitas informacinis punktas, kur galima gauti išsamesnės informacijos

3. Incidento, per kurį buvo pažeistas asmens duomenų saugumas, santrauka

4. Numanoma incidento data

5. Susijusių asmens duomenų pobūdis ir turinys, kaip nurodyta 3 straipsnio 2 dalyje

6. Tikėtinos asmens duomenų saugumo pažeidimo pasekmės susijusiam abonentui arba fiziniam asmeniui, kaip nurodyta 3 straipsnio 2 dalyje

7. Asmens duomenų saugumo pažeidimo aplinkybės, kaip nurodyta 3 straipsnio 2 dalyje

8. Priemonės, kurių dėl asmens duomenų saugumo pažeidimo ėmėsi teikėjas

9. Priemonės, kurių teikėjas rekomenduoja imtis, kad būtų sumažintas galimas neigiamas poveikis