Europos Parlamentas
2014-2019

PRIIMTI TEKSTAI

P8_TA(2018)0529

Japonijos užtikrinamo asmens duomenų apsaugos lygio tinkamumas

2018 m. gruodžio 13 d. Europos Parlamento rezoliucija dėl Japonijoje nustatytos asmens duomenų apsaugos tinkamumo (2018/2979(RSP))

Europos Parlamentas,

– atsižvelgdamas į Europos Sąjungos sutartį, Sutartį dėl Europos Sąjungos veikimo ir Europos Sąjungos pagrindinių teisių chartijos 6, 7, 8, 11, 16, 47 ir 52 straipsnius,

– atsižvelgdamas į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)[1] ir į kitus atitinkamus Europos duomenų apsaugos teisės aktus,

– atsižvelgdamas į 2015 m. spalio 6 d. Europos Sąjungos Teisingumo Teismo sprendimą byloje C-362/14 (Maximillian Schrems prieš Data Protection Commissioner)[2],

– atsižvelgdamas į 2016 m. gruodžio 21 d. Europos Teisingumo Teismo sprendimą Byloje C-203/15 (Tele2 Sverige AB prieš Post-och telestyrelsen) ir Byloje C-698/15 (Secretary of State for the Home Department prieš Tom Watson ir kitus)[3],

– atsižvelgdamas į savo 2017 m. gruodžio 12 d. rezoliuciją „Skaitmeninės prekybos strategijos kūrimas“[4],

– atsižvelgdamas į 2018 m. vasario 6 d. 29 straipsnio darbo grupės dokumentą „Tinkamumo kriterijai“[5], kuriame pateiktos Bendruoju duomenų apsaugos reglamentu (BDAR) pagrįstos gairės Komisijai ir Europos duomenų apsaugos valdybai dėl duomenų apsaugos lygio trečiosiose valstybėse ir tarptautinėse organizacijose vertinimo,

– atsižvelgdamas į 2018 m. gruodžio 5 d. Europos duomenų apsaugos valdybos nuomonę

---

1 OL L 119, 2016 5 4, p. 1.
2 ECLI:EU:C:2015:650.
3 ECLI:EU:C:2016:970.
4 OL C 369, 2018 10 11, p. 22.
5 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108; kuriam Europos duomenų apsaugos valdyba pritarė pirmajame plenariniame posėdyje.

dėl ES ir Japonijos sprendimo dėl tinkamumo projekto,

– atsižvelgdamas į Komisijos įgyvendinimo sprendimo pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl asmens duomenų tinkamos apsaugos Japonijoje projektą (COM(2018)XXXX),

– atsižvelgdamas į Piliečių laisvių, teisingumo ir vidaus reikalų komiteto (LIBE) *ad hoc* delegacijos 2017 m. spalio mėn. vizito į Japoniją, surengto vykdant derybas dėl tinkamumo, siekiant susitikti su atitinkamomis Japonijos valdžios institucijomis ir suinteresuotaisiais subjektais ir aptarti esminius elementus, į kuriuos Komisija turi atsižvelgti priimdama sprendimą dėl tinkamumo, išvadas,

– atsižvelgdamas į Darbo tvarkos taisyklių 123 straipsnio 2 dalį,

A. kadangi nuo 2018 m. gegužės 25 d. taikomas Bendrasis duomenų apsaugos reglamentas; kadangi Bendrojo duomenų apsaugos reglamento 45 straipsnio 2 dalyje nustatyti elementai, į kuriuos, vertindama apsaugos lygio trečiojoje valstybėje ar tarptautinėje organizacijoje tinkamumą, turi atsižvelgti Komisija;

B. kadangi Komisija visų pirma turi atsižvelgti į teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms, į atitinkamus bendruosius ir sektorių teisės aktus, įskaitant tuos, kurie susiję su visuomenės saugumu, gynyba, nacionaliniu saugumu, baudžiamąja teise ir valdžios institucijų prieiga prie asmens duomenų, taip pat į vienos ar daugiau nepriklausomų priežiūros institucijų egzistavimą ir sklandų veikimą ir trečiosios valstybės ar tarptautinės organizacijos prisiimtus tarptautinius įsipareigojimus;

C. kadangi Europos Teisingumo Teismas 2015 m. spalio 6 d. sprendime Byloje C-362/14 (Maximillian Schrems prieš Data Protection Commissioner) išaiškino, kad tinkamas apsaugos lygis trečiojoje valstybėje turi būti suprantamas kaip „iš esmės lygiavertis“ tam, kuris garantuojamas Europos Sąjungoje pagal Direktyvą 95/46/EB aiškinant ją vadovaujantis Chartija;

D. kadangi Japonija yra viena iš pagrindinių ES prekybos partnerių ir su ja ES neseniai sudarė ekonominės partnerystės susitarimą (EPS), kuriame įtvirtintos abiejų partnerių vertybės ir principai, kartu apsaugant ir joms opius klausimus; kadangi bendras pagrindinių teisių, įskaitant privatumą ir duomenų apsaugą, pripažinimas yra svarbus pagrindas priimant sprendimą dėl tinkamumo, kuris sudarys teisinį pagrindą perduoti asmens duomenis iš ES į Japoniją;

E. kadangi Piliečių laisvių, teisingumo ir vidaus reikalų komiteto *ad hoc* delegacija vizito metu į Japoniją pamatė Japonijos valdžios institucijų ir suinteresuotųjų subjektų suinteresuotumą ne tik taikyti pačias naujo Bendrojo duomenų apsaugos reglamento taisykles, bet ir sukurti patikimą ir itin kokybišką asmens duomenų perdavimo tarp ES ir Japonijos mechanizmą, kuris atitiktų ES teisinėje sistemoje reikalaujamas sąlygas, t. y. nustatyti apsaugos lygį, kuris iš esmės atitiktų ES duomenų apsaugos teisės aktuose numatytą apsaugos lygį;

F. kadangi, atsižvelgiant į vis didėjantį pasaulinės ekonomikos skaitmeninimą, asmens duomenų perdavimas tarp ES ir Japonijos komerciniais tikslais yra svarbus ES ir Japonijos santykių elementas; kadangi tokie duomenys turėtų būti perduodami visapusiškai paisant teisės į asmens duomenų apsaugą ir teisės į privatumą; kadangi

vienas iš pagrindinių ES tikslų yra ginti pagrindines teises, įtvirtintas Europos Sąjungos pagrindinių teisių chartijoje;

G. kadangi ES ir Japonija 2017 m. sausio mėn. pradėjo tartis, kaip palengvinti asmens duomenų perdavimą komerciniais tikslais taikant pirmą istorijoje išvadą dėl abipusio tinkamumo; kadangi Europos Parlamentas 2017 m. gruodžio 12 d. rezoliucijoje „Skaitmeninės prekybos strategijos kūrimas“ aiškiai „pripažįsta, kad sprendimai dėl tinkamumo [...] yra esminė priemonė siekiant užtikrinti asmens duomenų perdavimo iš ES į trečiąją šalį apsaugą“;

H. kadangi asmens duomenų perdavimui į Japoniją taikytinas sprendimas dėl tinkamumo būtų pirmas tokio pobūdžio sprendimas, priimtas pagal naujas griežtesnes Bendrojo duomenų apsaugos reglamento taisykles;

I. kadangi Japonija neseniai atnaujino ir sugriežtino savo duomenų apsaugos teisės aktus, siekdama suderinti juos su tarptautiniais standartais, ypač pagal naują Europos duomenų apsaugos teisės aktų sistemą nustatytomis apsaugos priemonėmis ir individualiomis teisėmis; kadangi Japonijos duomenų apsaugos teisinę sistemą sudaro įvairūs elementai, iš kurių svarbiausias yra Asmeninės informacijos apsaugos įstatymas;

J. kadangi 2018 m. birželio 12 d. Japonijos Ministrų kabinetas priėmė nutarimą, kuriuo Asmeninės informacijos apsaugos komisijai (PPC), kaip Asmeninės informacijos apsaugos įstatymo administravimo ir įgyvendinimo institucijai, deleguojami „įgaliojimai imtis reikiamų veiksmų, kad būtų suderinti Japonijos ir atitinkamos užsienio valstybės sistemų ir operacijų skirtumai, remiantis Įstatymo 6 straipsniu, siekiant užtikrinti tinkamą iš tokios šalies gautos asmeninės informacijos tvarkymą“; kadangi tame sprendime nustatyta, kad šie įgaliojimai apima PPC įgaliojimus sustiprinti apsaugą ir priimti griežtesnes taisykles, kurios papildytų Asmeninės informacijos apsaugos įstatymą ir Ministrų kabineto nutarimu nustatytas taisykles; kadangi, pagal šį sprendimą, minėtosios griežtesnės taisyklės Japonijos verslo subjektams būtų privalomos ir vykdytinos;

K. kadangi prie Komisijos įgyvendinimo sprendimo dėl tinkamos asmens duomenų apsaugos Japonijoje projekto kaip I priedas pridedamos 2018 m. birželio 15 d. PPC priimtos Papildomos taisyklės, pagrįstos Asmeninės informacijos apsaugos įstatymo 6 straipsniu, pagal kurį PPC aiškiai suteikiami įgaliojimai priimti griežtesnes taisykles, be kita ko, siekiant palengvinti tarptautinį duomenų perdavimą; kadangi Papildomos taisyklės dar nėra oficialiai paskelbtos;

L. kadangi šių Papildomų taisyklių paskirtis – išspręsti atitinkamų Japonijos ir ES duomenų apsaugos teisės aktų skirtumų problemas siekiant užtikrinti tinkamą sprendimu dėl tinkamumo pagrįstą iš ES gaunamų asmens duomenų tvarkymą, visų pirma taikytiną ypatingo dėmesio reikalaujančiai asmeninei informacijai (neskelbtiniems duomenims), saugomiems asmens duomenims, naudojimo paskirties nurodymui, su naudojimo paskirtimi susijusiam apribojimui, apribojimui teikti trečiajai šaliai kitoje valstybėje ir anonimiškai apdorotai informacijai;

M. kadangi Papildomos taisyklės būtų teisiškai privalomos visiems asmeninę informaciją tvarkantiems verslo subjektams, kurie gauna asmens duomenis, iš ES perduodamus remiantis sprendimu dėl tinkamumo, ir todėl privalo laikytis tų taisyklių, paisyti visų susijusių teisių ir vykdyti visas susijusias pareigas, ir jų vykdymą užtikrintų tiek PPC, tiek Japonijos teismai;

N. kadangi, siekiant užtikrinti iš esmės lygiavertį iš ES į Japoniją perduodamų asmens duomenų apsaugos lygį, Papildomomis taisyklėmis sukuriama papildoma apsauga, kuri turi būti taikoma nustatant griežtesnes iš ES perduodamų asmens duomenų tvarkymo sąlygas ar apribojimus, pavyzdžiui, kai perduodama ypatingo dėmesio reikalaujanti asmeninė informacija, kai asmens duomenys perduodami toliau, kai jie anoniminiai ar kai ribojama jų naudojimo paskirtis;

O. kadangi Japonijos duomenų apsaugos teisinėje sistemoje asmeninė informacija skiriasi nuo asmens duomenų ir kai kuriais atvejais reiškia tam tikros kategorijos asmens duomenis, konkrečiai saugomus asmens duomenis;

P. kadangi pagal Asmeninės informacijos apsaugos įstatymo 2 straipsnio 1 dalį „asmeninės informacijos“ sąvoka apima bet kokią su fiziniu asmeniu susijusią informaciją, pagal kurią galima nustatyti to asmens tapatybę; kadangi apibrėžtyje išskirtos dvi asmeninės informacijos kategorijos: i) asmens tapatybės kodai ir ii) kita asmeninė informacija, pagal kurią gali būti nustatyta asmens tapatybė; kadangi pastaroji kategorija apima informaciją, kuri, pati savaime, nepadeda nustatyti konkretaus asmens tapatybės, tačiau ją „lengvai susiejus“ su kita informacija, to asmens tapatybę nustatyti įmanoma;

Q. kadangi pagal Asmeninės informacijos apsaugos įstatymo 2 straipsnio 4 dalį „asmens duomenys“ – tai asmeninė informacija, sudaranti asmeninės informacijos duomenų bazę ir t.t.; kadangi Asmeninės informacijos apsaugos įstatymo 1 dalyje nurodoma, kad informacija tokiose duomenų bazėse sistemingai tvarkoma, ir tai yra panašu į „susisteminto rinkinio“ sąvoką pagal Bendrojo duomenų apsaugos reglamento 2 straipsnio 1 dalį; kadangi pagal Bendrojo duomenų apsaugos reglamento 4 straipsnio 1 dalį „asmens duomenys“ – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti; kadangi fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę galima nustatyti tiesiogiai arba netiesiogiai, visų pirma pagal identifikatorių, kaip antai vardą, pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius; kadangi sprendžiant, ar galima nustatyti fizinio asmens tapatybę, reikėtų atsižvelgti į visas priemones, pavyzdžiui, išskyrimą, kurias kaip pagrįstai tikėtina, asmens tapatybei tiesiogiai ar netiesiogiai nustatyti galėtų naudoti duomenų valdytojas ar kitas asmuo;

R. kadangi pagal Asmeninės informacijos apsaugos įstatymo 2 straipsnio 7 dalį „saugomi asmens duomenys“ – tai asmens duomenys, kuriuos asmens duomenis tvarkantis verslo subjektas turi teisę atskleisti, taisyti, papildyti arba ištrinti jų turinį, nustoti naudoti, ištrinti arba nustoti juos teikti trečiosioms šalims, ir kurie nėra nei duomenys, kurie pagal Ministrų kabineto įsakymą pripažinti duomenimis, galinčiais pakenkti viešiesiems ar kitiems interesams, jei sužinoma apie jų buvimą ar nebuvimą, nei duomenys, kurie turi būti panaikinti per ne ilgesnį kaip vienerių metų laikotarpį pagal Ministrų kabineto įsakymą; kadangi Papildomose taisyklėse sąvoka „saugomi asmens duomenys“ suderinama su sąvoka „asmens duomenys“, siekiant užtikrinti, kad tam tikri individualioms teisėms taikomi apribojimai nebūtų taikomi iš ES perduotiems duomenims;

S. kadangi į Japonijos duomenų apsaugos teisės, kuri aptariama įgyvendinimo sprendimo projekte, taikymo sritį nepatenka keli sektoriai, kai juose asmens duomenys tvarkomi konkrečiais tikslais; kadangi įgyvendinimo sprendimo projektas nebūtų taikomas

asmens duomenų perdavimui iš ES gavėjui, kuriam taikoma kuri nors iš pirmiau minėtų išimčių, nustatytų Japonijos duomenų apsaugos teisės aktuose;

T. kadangi, kalbant apie tolesnį ES asmens duomenų perdavimą iš Japonijos į trečiąją šalį, įgyvendinimo sprendimo projekte nenumatyta galimybė, vykdant tokius tolesnius perdavimus, naudoti perdavimo priemones, kuriomis nesukuriami saistantys Japonijos duomenų eksportuotojo ir trečiosios šalies duomenų importuotojo santykiai ir neužtikrinamas reikalaujamas apsaugos lygis; kadangi toks atvejis būtų, pavyzdžiui, Azijos ir Ramiojo vandenyno šalių ekonominio bendradarbiavimo tarpvalstybinio privatumo taisyklių (angl. APEC CBPR) sistema, kurioje dalyvauja Japonija, nes šioje sistemoje apsaugos nelemia eksportuotojo ir importuotojo dvišalių santykių kontekste sudarytas saistantis susitarimas ir duomenų apsauga yra akivaizdžiai žemesnio lygio nei ta, kuri užtikrinama Asmeninės informacijos apsaugos įstatymu ir Papildomomis taisyklėmis kartu;

U. kadangi Europos duomenų apsaugos valdyba savo 2018 m. gruodžio 5 d. nuomonėje, remdamasi Komisijos pateiktais dokumentais, įvertina, ar Japonijos duomenų apsaugos teisinė sistema suteikia pakankamas asmenų duomenų apsaugos garantijas; kadangi Europos duomenų apsaugos valdyba palankiai vertina Komisijos ir Asmeninės informacijos apsaugos komisijai (PPC) pastangas didinti Japonijos ir Europos teisinių sistemų konvergenciją, siekiant palengvinti asmens duomenų perdavimą; kadangi Europos duomenų apsaugos valdyba pripažįsta, kad Papildomose taisyklėse numatyti patobulinimai, siekiant pašalinti kai kuriuos šių dviejų sistemų skirtumus yra labai svarbūs ir geri; kadangi ji pažymi, jog išlieka keletas susirūpinimą keliančių klausimų, pavyzdžiui, asmens duomenų, perduotų iš ES į Japoniją per visą jų gyvavimo ciklą, apsauga, ir rekomenduoja, kad Komisija pateiktų daugiau įrodymų ir paaiškinimų dėl iškeltų klausimų ir atidžiai stebėtų, ar taisyklės taikomos veiksmingai;

V. kadangi kartu su įgyvendinimo sprendimo projektu pateikiamas 2018 m. rugsėjo 14 d. teisingumo ministro raštas, kuriame daroma nuoroda į Teisingumo ministerijos ir kelių kitų ministerijų bei agentūrų parengtą dokumentą „Japonijos valdžios institucijų vykdomas asmeninės informacijos rinkimas ir naudojimas baudžiamosios teisės vykdymo ir nacionalinio saugumo užtikrinimo tikslais“, kuriame pateikiama taikomos teisinės sistemos apžvalga ir Komisijai nurodomos oficialiosios atstovybės, garantijos ir įsipareigojimai, pasirašyti aukščiausiu ministrų ir agentūrų lygmeniu, kurie pridedami kaip įgyvendinimo sprendimo II priedas;

1. atkreipia dėmesį į išsamią analizę, kurią Komisija pateikė savo įgyvendinimo sprendimo dėl asmens duomenų apsaugos projekte, įskaitant priežiūros ir teisių gynimo mechanizmus, taikomus komercinės veiklos vykdytojų vykdomam duomenų tvarkymui, taip pat Japonijos valdžios institucijų prieigai prie duomenų, visų pirma teisėsaugos ir nacionalinio saugumo srityse;

2. atkreipia dėmesį, kad Japonija tuo pat metu rengia ir asmens duomenų, kuriuos Japonija perduoda ES pagal Asmeninės informacijos apsaugos įstatymo 23 straipsnį, apsaugos lygio pripažinimą – tai būtų pirma abipusė tinkamumo išvada pasaulyje, kuria remiantis būtų galima sukurti didžiausią pasaulyje laisvų ir saugių duomenų srautų erdvę;

3. palankiai vertina šį pokytį kaip aukštų duomenų apsaugos standartų sklaidos pasaulyje išraišką; vis dėlto atkreipia dėmesį, kad dėl to jokiu būdu ES sprendimuose dėl tinkamumo neturėtų būti taikomas principas „akis už akį“; primena, kad priimdama sprendimą dėl tinkamumo pagal Bendrąjį duomenų apsaugos reglamentą Komisija turi

objektyviai įvertinti teisinę ir praktinę padėtį trečiojoje šalyje, teritorijoje, sektoriuje ar tarptautinėje organizacijoje;

4. atkreipia dėmesį į tai, kad Europos Teisingumo Teismas nusprendė, jog pagal sąvoką „tinkamas apsaugos lygis“ nereikalaujama tokio paties apsaugos lygio, kuris garantuojamas ES, bet ji turi būti suprantama kaip reikalavimas, kad trečioji šalis, atsižvelgdama į savo vidaus teisę arba tarptautinius įsipareigojimus, užtikrintų pagrindinių teisių ir laisvių, kurios iš esmės yra lygiavertės Europos Sąjungoje garantuojamoms pagal Bendrąjį duomenų apsaugos reglamentą, apsaugos lygį, kuris nustatomas atsižvelgiant į Chartiją“;

5. pažymi, kad teisė į privatumą ir asmens duomenų apsaugą užtikrinama konstituciniu lygmeniu tiek Japonijoje, tiek ES, tačiau visiškas ES ir Japonijos taisyklių suderinimas neįmanomas dėl konstitucinės struktūros ir kultūros skirtumų;

6. atkreipia dėmesį į Asmeninės informacijos apsaugos įstatymo pakeitimus, kurie įsigaliojo 2017 m. gegužės 30 d.; palankiai vertina esminius patobulinimus;

7. pažymi, kad į APPI materialinę taikymo sritį nepatenkančių kategorijų verslo ir perdirbimo veikla aiškiai neįtraukiama į tinkamumo išvados taikymo sritį;

8. mano, kad priėmus iš dalies pakeistą Asmeninės informacijos apsaugos įstatymą ir 2016 m. priėmus BDAR, Japonijos ir ES duomenų apsaugos sistemos pasižymi aukštu suderinimo lygiu principų, apsaugos priemonių ir asmens teisių, taip pat priežiūros ir vykdymo užtikrinimo mechanizmų požiūriu; visų pirma atkreipia dėmesį į nepriklausomos priežiūros institucijos (PPC) sukūrimą iš dalies pakeitus Asmeninės informacijos apsaugos įstatymą;

9. vis dėlto pažymi, kad pačios PPC manymu nepaisant aukšto abiejų sistemų suderinimo lygio, esama tam tikrų svarbių skirtumų; taip pat pažymi, kad siekdama užtikrinti aukštesnį iš ES perkeliamų asmens duomenų apsaugos lygį, 2018 m. birželio 15 d. PPC patvirtino Papildomas taisykles;

10. palankiai vertina keletą svarbių Papildomų taisyklių išaiškinimų, įskaitant „anonimizuotos asmeninės informacijos“ sąvokos Asmeninės informacijos apsaugos įstatyme suderinimą su „anonimiškos informacijos“ apibrėžtimi Bendrajame duomenų apsaugos reglamente;

11. mano, jog atsižvelgiant į tai, kad Papildomų taisyklių papildomos apsaugos priemonės taikomos tik duomenų perdavimui pagal sprendimus dėl tinkamumo; primena, kad, atsižvelgiant į sprendimo dėl tinkamumo taikymo sritį, kai kurie duomenų perdavimai bus atliekami pagal tuos kitus turimus mechanizmus;

12. pripažįsta, kad papildomos apsaugos priemonės, numatytos Papildomose taisyklėse, apsiriboja tik iš Europos perduodamais asmens duomenimis, todėl verslo subjektai, kurie tuo pačiu metu tvarko Japonijos ir Europos asmens duomenis, privalės laikytis Papildomų taisyklių, užtikrindami, pvz., technines (ženklinimo) ar organizacines priemones (pvz., saugoti specialioje duomenų bazėje), kad galėtų identifikuoti tokius asmens duomenis per visą jų gyvavimo ciklą; ragina Komisiją stebėti padėtį, siekiant išvengti galimų spragų, leidžiančių veiklos vykdytojams apeiti Papildomose taisyklėse nustatytas pareigas perduodant duomenis per trečiąsias šalis;

13. pažymi, kad „asmens duomenų“ apibrėžtis Asmeninės informacijos apsaugos įstatyme

neapima duomenų, „ministrų kabineto įsakymu pripažintų kaip turinčių nedaug galimybių pakenkti asmens teisėms ir interesams, atsižvelgiant į jų naudojimo būdą“; primygtinai ragina Komisiją įvertinti, ar šis žalos vertinimu grindžiamas metodas yra suderinamas su ES požiūriu, pagal kurį bet koks asmens duomenų tvarkymas patenka į duomenų apsaugos teisės taikymo sritį; tačiau taip pat pažymi, kad toks požiūris taikytinas labai retais atvejais;

14. be to, pažymi, kad „asmeninės informacijos“ apibrėžtis Asmeninės informacijos apsaugos įstatyme apima tik informaciją, „pagal kurią galima nustatyti konkretaus asmens tapatybę“; taip pat pažymi, kad į šią apibrėžtį neįtrauktas Bendrajame duomenų apsaugos reglamente pateiktas paaiškinimas, jog asmeninė informacija taip pat turėtų būti laikoma asmens duomenimis tais atvejais, kai ji gali būti naudojama tik asmeniui „išskirti“, kaip aiškiai nustatė Europos Sąjungos Teisingumo Teismas;

15. yra susirūpinęs dėl to, kad Asmeninės informacijos apsaugos įstatyme pateikta siauresnė „asmens duomenų“ apibrėžtis (pagrįsta „asmeninės informacijos“ apibrėžtimi) gali neatitikti standarto, t. y. nebus „iš esmės lygiavertė“ apibrėžčiai, nustatytai Bendrajam duomenų apsaugos reglamente, ir gali neatitikti Europos Sąjungos Teisingumo Teismo praktikos; todėl abejoja įgyvendinimo sprendimo projekto teiginiu, kad „pagal Asmeninės informacijos apsaugos įstatymą ES duomenys visada pateks į „asmens duomenų“ kategoriją“; ragina Komisiją atidžiai stebėti skirtingų sąvokų praktinį poveikį priimant sprendimą dėl tinkamumo ir jį periodiškai peržiūrint;

16. ragina Komisiją pateikti tolesnius paaiškinimus ir, jei būtina, iš Japonijos pareikalauti tolesnių privalomų papildomų taisyklių, siekiant užtikrinti, kad visi asmens duomenys, kaip apibrėžta Bendrajame duomenų apsaugos reglamente, būtų apsaugoti juos perduodant Japonijai;

17. susirūpinęs pažymi, kad, kitaip nei ES teisės aktuose, nei Asmeninės informacijos apsaugos įstatyme, nei Asmeninės informacijos apsaugos komisijos gairėse nėra teisinių nuostatų dėl automatizuoto sprendimų priėmimo ir profiliavimo ir kad šis klausimas sprendžiamas tik tam tikrose konkrečių sektorių taisyklėse, nenumatant išsamios bendros teisinės sistemos, kuria būtų nustatyta esminė ir tvirta apsauga nuo automatizuoto sprendimų priėmimo ir profiliavimo; ragina Komisiją parodyti, ar Japonijos duomenų apsaugos sistemoje šis klausimas sprendžiamas taip, kad būtų užtikrintas lygiavertis apsaugos lygis; mano, kad tai ypač svarbu atsižvelgiant į naujausius „Facebook“ ir „Cambridge Analytica“ profiliavimo atvejus;

18. mano, jog atsižvelgiant į Europos duomenų apsaugos valdybos tinkamumo kriterijus ir į tai, kad APPI nėra konkrečių nuostatų, reikia tolesnių išsamių paaiškinimų dėl tiesioginės rinkodaros norint įrodyti Japonijos asmens duomenų apsaugos lygiavertiškumą;

19. atkreipia dėmesį į Europos duomenų apsaugos valdybos nuomonę, kurioje nurodomi keli susirūpinimą keliantys klausimai, pvz., asmens duomenų, perduotų iš ES į Japoniją per visą jų gyvavimo ciklą, apsauga; ragina Komisiją įgyvendinimo sprendime tinkamai nurodyti ir pateikti papildomus įrodymus ir paaiškinimus, iš kurių būtų matyti, kad egzistuoja tinkamos apsaugos priemonės;

20. ragina Komisiją paaiškinti, ar, kalbant apie tolesnio duomenų perdavimo klausimą, Papildomose taisyklėse pateiktame sprendime, pagal kurį reikalaujama išankstinio ES duomenų subjektų sutikimo dėl tolesnio duomenų perdavimo trečiajai šaliai užsienio

valstybėje, trūksta tam tikrų esminių elementų, kurie leistų duomenų subjektams suformuluoti savo sutikimą, nes jame nėra aiškiai apibrėžta, ką apima sąvoka „informacija apie aplinkybes, susijusias su perdavimu, dėl kurio [duomenų subjektui] reikia priimti sprendimą duoti savo sutikimą“, laikantis Bendrojo duomenų apsaugos reglamento 13 straipsnio, pavyzdžiui, tolesnio duomenų perdavimo paskirties trečioji šalis; ragina Komisiją išsamiau paaiškinti, kokių pasekmių gali tikėtis duomenų subjektas, atsisakęs duoti sutikimą tolesniam savo asmens duomenų perdavimui;

21. apgailestauja dėl to, kad, kalbant apie veiksmingą Asmeninės informacijos apsaugos įstatymo vykdymo užtikrinimą, galimų baudų, kurias nustatytų baudžiamosios institucijos, dydis yra nepakankamas norint užtikrinti veiksmingą šio įstatymo laikymąsi, nes baudos neatrodo proporcingos, veiksmingos ar atgrasančios palyginti su pažeidimo sunkumu; vis dėlto pažymi, kad Asmeninės informacijos apsaugos įstatyme taip pat numatytos baudžiamosios sankcijos, įskaitant laisvės atėmimą; ragina Komisiją pateikti informaciją apie faktinį administracinių baudų ir baudžiamųjų sankcijų taikymą praeityje;

22. atkreipia dėmesį į tai, kad, nors Asmeninės informacijos apsaugos komisija negali prižiūrėti teisėsaugos sektoriaus vykdomos duomenų tvarkymo veiklos, yra kitų priežiūros mechanizmų, įskaitant nepriklausomos prefektūros viešojo saugumo komisijos vykdomą priežiūrą; pažymi, kad Informacijos atskleidimo ir asmeninės informacijos apsaugos peržiūros valdyba taip pat turi tam tikrą kompetenciją šioje srityje, įskaitant prašymų dėl prieigos peržiūrą ir nuomonių skelbimą, tačiau atkreipia dėmesį į tai, kad šie įgaliojimai nėra teisiškai privalomi; palankiai vertina tai, kad ES ir Japonija susitarė taikyti specialų teisių gynimo mechanizmą, kurį administruotų ir prižiūrėtų Asmeninės informacijos apsaugos komisija ir kuris būtų taikomas asmens duomenų tvarkymui teisėsaugos ir nacionalinio saugumo sektoriuose;

23. pažymi, kad, remiantis Japonijos įstatymu dėl administracinių įstaigų turimos asmeninės informacijos apsaugos, verslo subjektai taip pat gali „savanorišku pagrindu“ perduoti duomenis teisėsaugos institucijoms; pabrėžia, jog tai nėra numatyta Bendrajame duomenų apsaugos reglamente arba Policijos direktyvoje, ir ragina Komisiją įvertinti, ar tai suderinama su buvimo „iš esmės lygiaverčiu“ Bendrajam duomenų apsaugos reglamentui standartu;

24. yra susipažinęs su žiniasklaidos pranešimais apie Japonijos signalų žvalgybos direktoratą (DFS), kuriame dirba apie 1 700 žmonių ir kuris turi bent šešis stebėjimo įrenginius, leidžiančius visą parą slapta klausytis telefono skambučių, skaityti e. laiškus ir kitas ryšių priemones[1]; nerimauja dėl to, kad apie šį nediferencijuoto masinio sekimo elementą įgyvendinimo sprendimo projekte net neužsimenama; ragina Komisiją pateikti daugiau informacijos apie Japonijos vykdomą masinį sekimą; reiškia didelį susirūpinimą, kad dėl šio masinio sekimo bus neįmanoma užtikrinti atitikties kriterijams, kuriuos Europos Sąjungos Teisingumo Teismas nustatė sprendime Schrems (Byla C-362/14);

25. apgailestauja dėl to, kad į įgyvendinimo sprendimo projekto II priedą įtrauktas dokumentas „Japonijos valdžios institucijų vykdomas asmeninės informacijos rinkimas ir naudojimas baudžiamosios teisės ir nacionalinio saugumo tikslais“, neturi tokios pat

---

[1] Ryan Gallagher, „The Untold Story of Japan’s Secret Spy Agency“, The Intercept, 2018 m. gegužės 19 d., https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/

privalomos teisinės galios kaip Papildomos taisyklės;

Išvados

26. ragina Komisiją pateikti daugiau įrodymų ir paaiškinimų minėtais klausimais, įskaitant klausimus, akcentuotus Europos duomenų apsaugos valdybos savo 2018 m. gruodžio 5 d. nuomonėje, siekiant parodyti, kad Japonijos duomenų apsaugos teisinėje sistemoje užtikrinamas tinkamas apsaugos lygis, kuris yra iš esmės lygiavertis Europos duomenų apsaugos teisinėje sistemoje nustatytam apsaugos lygiui;

27. mano, kad šis sprendimas dėl tinkamumo taip pat gali pasiųsti stiprų signalą viso pasaulio šalims, kad panašių į aukštus ES duomenų apsaugos standartus laikymasis duoda labai apčiuopiamų rezultatų; atsižvelgdamas į tai, pabrėžia, kad šis sprendimas dėl tinkamumo yra svarbus kaip precedentas būsimoms partnerystėms su kitomis šalimis, kurios priėmė šiuolaikinius duomenų apsaugos teisės aktus;

28. paveda Piliečių laisvių, teisingumo ir vidaus reikalų komitetui toliau stebėti pokyčius šioje srityje, įskaitant Teisingumo Teisme nagrinėjamas bylas, ir stebėti tolesnius veiksmus, susijusius su šioje rezoliucijoje pateiktomis rekomendacijomis;

°

° °

29. paveda Pirmininkui perduoti šią rezoliuciją Tarybai, Komisijai, valstybių narių vyriausybėms ir parlamentams, Europos duomenų apsaugos valdybai, Europos duomenų apsaugos priežiūros pareigūnui, pagal Bendrojo duomenų apsaugos reglamento 93 straipsnio 1 dalį įsteigtam komitetui, Europos Tarybai ir Japonijos vyriausybei.