Nuomonė 32/2021 dėl Europos Komisijos įgyvendinimo sprendimo pagal reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Korėjos Respublikoje projekto

Versija 1.0

Priimta 2021 m. rugsėjo 24 d.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

TURINYS

Europos duomenų apsaugos valdyba,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – **BDAR**) 70 straipsnio 1 dalies s punktą,

atsižvelgdama į Europos ekonominės erdvės (toliau – **EEE**) susitarimą, ypač į jo XI priedą ir 37 protokolą su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[1],

atsižvelgdama į Darbo tvarkos taisyklių 12 ir 22 straipsnius,

PRIĖMĖ ŠIĄ NUOMONĘ:

1. SANTRAUKA

1. 2021 m. birželio 16 d. Europos Komisija pradėjo oficialų šio įgyvendinimo sprendimo projekto (toliau – **sprendimo projektas**) dėl tinkamos asmens duomenų apsaugos Korėjos Respublikoje priėmimo procesą pagal Asmens duomenų apsaugos aktą pagal BDAR[2].

2. Tą pačią dieną Europos Komisija paprašė Europos duomenų apsaugos valdybos (toliau – **EDAV**)[3] pateikti savo nuomonę. EDAV įvertino Korėjos Respublikos užtikrinamo apsaugos lygio tinkamumą, remdamasi paties sprendimo projekto nagrinėjimu, taip pat Europos Komisijos pateiktų[4] dokumentų analize.

3. EDAV didžiausią dėmesį skyrė ir bendrųjų BDAR aspektų sprendimo projekte, ir valdžios institucijų prieigos prie asmens duomenų, perduotų iš EEE teisėsaugos ir nacionalinio saugumo tikslais, įskaitant teisių gynimo priemones, kuriomis gali pasinaudoti EEE asmenys, vertinimui. Taip pat EDAV įvertino, ar Korėjos teisinėje sistemoje yra įdiegtos numatytos apsaugos priemonės ir ar jos veiksmingos.

4. Šiam darbui atlikti EDAV kaip pagrindu naudojosi savo 2018 m. vasario mėn. priimtu BDAR darbiniu dokumentu dėl referencinio tinkamumo[5] (toliau – **BDAR darbinis dokumentas dėl referencinio tinkamumo**) ir EDAV rekomendacijomis Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones[6].

1.1. Sritys, dėl kurių sutariama

5. Pagrindinis EDAV tikslas – pateikti nuomonę Europos Komisijai dėl asmenims, kurių asmens duomenys yra perduodami Korėjos Respublikai, suteikiamo apsaugos lygio tinkamumo. Svarbu pripažinti, kad EDAV nesitiki, jog Korėjos duomenų apsaugos sistemoje bus atkartoti Europos duomenų apsaugos teisės aktai.

[1] Šioje nuomonėje daromos nuorodos į **valstybes nares** turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.
[2] Žr. pranešimą spaudai https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ten pat.
[4] EDAV savo analizę atliko remdamasi Korėjos vyriausybės parengtais oficialiais vertimais.
[5] WP254, 2018 m. vasario 6 d. BDAR darbinis dokumentas dėl referencinio tinkamumo, (kurį patvirtino EDAV, žr. https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Žr. 2020 m. lapkričio 10 d. priimtas EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

6. Vis dėlto EDAV primena, kad tam, jog ši sistema būtų laikoma užtikrinančia tinkamą apsaugos lygį, BDAR 45 straipsnyje ir Europos Sąjungos Teisingumo Teismo (toliau – **ESTT**) praktikoje reikalaujama, kad trečiosios šalies teisės aktai būtų suderinti su BDAR įtvirtintais pagrindiniais principais. Atsižvelgiant į tai, Korėjos duomenų apsaugos sistemoje yra daug panašumų su Europos duomenų apsaugos sistema, t. y. ji turi vieną pagrindinį teisės aktą, apimantį tiek viešąjį, tiek privatųjį sektorių, kuris papildytas konkretiems sektoriams skirtais teisės aktais.

7. Kalbant apie turinį, EDAV pažymi, kad yra svarbių sričių, kuriose BDAR sistema ir Korėjos duomenų apsaugos sistema yra suderintos, atsižvelgiant į tam tikras pagrindines nuostatas, pavyzdžiui, sąvokas (pvz., „asmens duomenys“, „tvarkymas“, „duomenų subjektas“); teisėto ir sąžiningo duomenų tvarkymo teisėtais tikslais pagrindus; tikslų apribojimą; duomenų kokybę ir proporcingumą, duomenų saugojimą, saugumą ir konfidencialumą; skaidrumą ir specialiųjų kategorijų duomenis.

8. Be to, kas išdėstyta pirmiau, EDAV palankiai vertina Europos Komisijos ir Korėjos valdžios institucijų pastangas užtikrinti, kad Korėjos Respublika suteiktų tinkamą apsaugos lygį, prilygstantį BDAR užtikrinamam apsaugos lygiui, priimdama Korėjos priežiūros institucijos pranešimus (taikytinus ne tik iš EEE Korėjai perduotiems asmens duomenims), siekiant užpildyti atotrūkį tarp BDAR ir Korėjos duomenų apsaugos sistemos. Atsižvelgiant į tai, EDAV nori pabrėžti šių pranešimų svarbą vertinant Korėjos Respublikos sistemos tinkamumą, nurodydama, kad, pavyzdžiui, juose pateikiami aktualūs kai kurių svarbių apsaugos priemonių paaiškinimai, be kita ko, susiję su PIPA išimčių, taikomų pseudoniminiams asmens duomenims tvarkyti mokslo, tyrimų ir statistikos tikslais, taikymo sritimi, tolesniu perdavimu ir taisyklėmis, taikomomis valdžios institucijų prieigai prie duomenų.

1.2. Iššūkiai

9. Nors EDAV nustatė, kad daugelis Korėjos duomenų apsaugos sistemos aspektų iš esmės yra lygiaverčiai Europos duomenų apsaugos sistemai, ji taip pat padarė išvadą, kad yra tam tikrų aspektų, kuriuos gali prireikti panagrinėti atidžiau ir juos patikslinti. Konkrečiai, EDAV mano, kad siekiant, jog būtų užtikrintas iš esmės lygiavertis apsaugos lygis, reikėtų išsamiau įvertinti šiuos klausimus ir juos turėtų atidžiai stebėti Europos Komisija.

1.2.1. Bendroji informacija

10. EDAV atsižvelgia į tai, kad Pranešimas Nr. 2021-1 *turi administracinės taisyklės, turinčios teisiškai privalomą galią asmens duomenų valdytojui, statusą, nes bet koks pranešimo pažeidimas gali būti laikomas atitinkamų PIPA nuostatų pažeidimu*[7]. Tačiau, atsižvelgiant į tai, kad į pranešimą neįtrauktos papildomos taisyklės *per se*, o veikiau paaiškinimai, kaip turėtų būti suprantamas teisės aktais nustatytas PIPA tekstas, kad būtų galima jį taikyti, ir atsižvelgiant į jo bendrą svarbą, ypač dėl PIPA pseudoniminimo nuostatų, kurios, kaip supranta EDAV, yra vykstančių teisminių bylų objektas, EDAV ragina Europos Komisiją pateikti daugiau informacijos apie Pranešimo Nr. 2021-1 privalomumą, įgyvendinamumą ir galiojimą ir rekomenduotų atidžiai stebėti, kaip jo laikomasi praktikoje, ypač atsižvelgiant į tai, kad jį taiko ne tik Korėjos priežiūros institucija, bet ir teismai, ypač tais atvejais, kai lygiavertis apsaugos lygis, kurį suteikia Korėjos teisinė sistema, grindžiamas jame pateiktais paaiškinimais.

1.2.2. Bendrieji duomenų apsaugos aspektai

11. Kalbant apie sprendimo dėl tinkamumo taikymo sritį, EDAV pažymi, kad ji apims duomenų perdavimą iš EEE teisinės sistemos tiek viešiesiems, tiek privatiesiems „asmens duomenų valdytojams“, kuriems taikomas PIPA. EDAV supranta, kad į šią sąvoką yra įtraukti subjektai, pagal BDAR veikiantys kaip

[7] Žr. sprendimo projekto I priedo I skyrių.

duomenų tvarkytojai, tačiau, siekiant išvengti nesusipratimų, ji ragina Europos Komisiją patikslinti, kad sprendimas dėl tinkamumo taip pat apims duomenų perdavimą „tvarkytojams“ Korėjoje.

12. Svarbus aspektas, į kurį EDAV norėtų atkreipti dėmesį, yra susijęs su pseudoniminės informacijos sąvoka Korėjos duomenų apsaugos sistemoje. Pagal Korėjos įstatymus, pseudoniminių asmens duomenų tvarkymui taikomos kelių atitinkamų nuostatų, įskaitant tas, kurios susijusios su individualiomis duomenų subjekto teisėmis ir duomenų saugojimu, išimtys. Europos Komisijos teigimu, taip yra tik tuo atveju, kai pseudoniminiai asmens duomenys yra tvarkomi statistikos, mokslinių tyrimų ar archyvavimo tikslais dėl viešojo intereso. Tačiau šį teiginį iš esmės patvirtina Pranešimas Nr. 2021-1, dėl kurio jau minėtas papildomos informacijos apie šio pranešimo privalomumą, įgyvendinamumą ir galiojimą poreikis bei jų stebėjimas šiomis aplinkybėmis tampa labai svarbūs. Be to, EDAV ragina Europos Komisiją toliau vertinti pseudonimų suteikimo poveikį pagal Korėjos teisę ir, svarbiausia, kaip tai gali paveikti duomenų subjektų, kurių asmens duomenys perduodami Korėjos Respublikai pagal sprendimą dėl tinkamumo, pagrindines teises ir laisves. Visų pirma EDAV ragina Europos Komisiją toliau vertinti PIPA 28 straipsnio 7 dalyje ir CIA 40 straipsnio 3 dalyje numatytas nukrypti leidžiančias nuostatas ir atidžiai stebėti jų taikymą bei atitinkamą teismų praktiką, kad būtų galima užtikrinti, kad duomenų subjekto teisės nebūtų nepagrįstai apribotos, kai asmens duomenys, perduoti pagal sprendimą dėl tinkamumo, yra tvarkomi šiais tikslais.

13. Taip pat EDAV pažymi, kad pagal Korėjos įstatymus teisė atšaukti sutikimą galioja tik tam tikromis aplinkybėmis, todėl ragina Europos Komisiją išsamiau įvertinti bendrosios teisės atšaukti sutikimą nebuvimo poveikį ir pateikti papildomų garantijų, kad būtų užtikrinta, kad esminis duomenų apsaugos lygis būtų garantuojamas bet kuriuo metu, taip pat, prireikus, išaiškinant teisės sustabdyti duomenų tvarkymą laikantis PIPA vaidmenį, kai nėra bendrosios teisės atšaukti sutikimą.

14. Kalbat apie tolesnį duomenų perdavimą, EDAV pripažįsta, kad informacija grindžiamas duomenų subjekto sutikimas paprastai bus naudojamas kaip duomenų perdavimo iš asmens duomenų valdytojo Korėjoje duomenų gavėjui trečiojoje šalyje pagrindas ir kad Pranešime Nr. 2021-1 numatyta, jog asmenys turi būti informuoti apie trečiąją šalį, kuriai bus pateikti jų duomenys. Tačiau EDAV ragina Europos Komisiją užtikrinti, kad į duomenų subjektui teikiamą informaciją taip pat būtų įtraukta informacija apie galimą perdavimo riziką, kylančią dėl to, kad trečiojoje šalyje nėra tinkamos apsaugos, taip pat dėl to, kad nėra tinkamų apsaugos priemonių. Be to, EDAV palankiai vertintų, jei sprendime dėl tinkamumo būtų patvirtinimas, kad asmens duomenys nebus perduodami iš Korėjos asmens duomenų valdytojų į trečiąją šalį bet kokioje situacijoje, kurioje pagal BDAR negalėtų būti duodamas galiojantis sutikimas, pvz., dėl galios disbalanso.

15. Kalbant apie Korėjos priežiūros institucijos narių skyrimą, nors oficiali procedūra atitiktų BDAR ir todėl duotų teigiamus lygiavertiškumo su EEE teisine sistema tikrinimo rezultatus, EDAV palankiai vertintų, jei Europos Komisija stebėtų bet kokius pokyčius, kurie gali turėti įtakos Pietų Korėjos priežiūros institucijos narių nepriklausomumui.

16. Kalbant apie biudžetą, vėlgi remiantis Europos Komisijos pateikta informacija, nenurodomi nei į PIPC paskirtų darbuotojų ypatumai, nei jai skirti finansiniai ištekliai. Todėl EDAV norėtų, kad sprendimo projekte būtų pateikta papildoma informacija šiomis dviem aktualiomis temomis.

1.2.3. Dėl valdžios institucijų prieigos prie duomenų, perduotų Korėjos Respublikai

17. EDAV taip pat analizavo Korėjos teisinę sistemą, susijusią su vyriausybės prieiga teisėsaugos ir nacionalinio saugumo tikslais prie asmens duomenų, perduodamų iš EEE į Korėją. Nors pripažindama Korėjos vyriausybės pateiktus pareiškimus ir patikinimus, kaip nurodyta sprendimo projekto II priede, EDAV nustatė keletą aspektų, kuriuos reikia patikslinti arba kurie kelia klausimų.

18. EDAV pažymi, kad PIPA nuostatos teisėsaugos srityje taikomos be apribojimų. EDAV taip pat pažymi, kad duomenų tvarkymui nacionalinio saugumo srityje taikomas labiau ribotas PIPA įtvirtintų nuostatų rinkinys.

19. Kalbant apie telekomunikacijos paslaugų teikėjų savanorišką asmens duomenų atskleidimą nacionalinėms saugumo institucijoms, EDAV yra susirūpinusi, kad ryšys tarp sprendimo projekto I priedo 3 skyriaus, kuriame nurodoma, kad paslaugų teikėjai iš esmės turi pranešti atitinkamam asmeniui, kai jie savanoriškai vykdo prašymą, ir PIPA 58 straipsnio 1 dalies 2 punkto, t. y. dalinės išimties nacionalinio saugumo tikslais, yra neaiškus. Dėl to informacijos reikalavimai gali tapti neveiksmingais ir duomenų subjektams bus žymiai sunkiau ginti savo teises į duomenų apsaugą, ypač kalbant apie apskundimą teismine tvarka.

20. Nors sprendimo projekte nėra aiškiai nurodyta, EDAV iš Europos Komisijos pateiktų paaiškinimų supranta, kad pagal Korėjos teisinę sistemą draudžiama masiškai perimti telekomunikacijos duomenis. Todėl naujausia Europos Žmogaus Teisių Teismo (toliau – **EŽTT**) praktika dėl masinio perėmimo tvarkos neturės tiesioginės reikšmės duomenų apsaugos lygio Korėjoje vertinimui.

21. Sprendimo projekte nėra jokios informacijos apie tolesnio duomenų perdavimo teisinę sistemą nacionalinio saugumo srityje. Nors EDAV suprato, kad, Europos Komisijos požiūriu, tolesnį duomenų perdavimą nacionalinio saugumo tikslais pakankamai reglamentuoja konstitucinėje sistemoje ir PIPA nustatytos bendrosios apsaugos priemonės ir principai, EDAV yra susirūpinusi dėl to, ar gali būti laikoma, kad tai atitinka teisės tikslumo ir aiškumo reikalavimus ir įtvirtina veiksmingas ir vykdytinas apsaugos priemones. Apsaugos priemonės, kurias nurodo Europos Komisija yra labai bendro pobūdžio ir teisiniame pagrinde nėra nagrinėjamos konkrečios aplinkybės bei sąlygos, kuriomis gali būti vykdomas tolesnis duomenų perdavimas nacionalinio saugumo tikslais. Šiomis aplinkybėmis EDAV taip pat pažymi, kad Europos Komisija neatsižvelgė į tai, jog tarp Korėjos Respublikos ir trečiųjų šalių ar tarptautinių organizacijų yra sudaryti tarptautiniai susitarimai, kuriuose gali būti numatytos konkrečios nuostatos dėl teisėsaugos ir (arba) žvalgybos tarnybų tarptautinio asmens duomenų perdavimo trečiosioms šalims. EDAV mano, kad dvišalių ar daugiašalių susitarimų sudarymas su trečiosiomis šalimis teisėsaugos ar žvalgybos bendradarbiavimo tikslais, tikėtina, darys poveikį vertinamai Korėjos duomenų apsaugos teisinei sistemai.

22. EDAV pažymi, kad baudžiamosios teisėsaugos ir nacionalinių saugumo institucijų priežiūrą užtikrina įvairių vidaus ir išorės institucijų, visų pirma PIPC, kuri turi pakankamai vykdomųjų įgaliojimų, grupė.

23. Norint, kad taisomieji veiksmai ir teisių gynimas būtų veiksmingi, reikia, kad duomenų subjektai galėtų kreiptis į kompetentingą įstaigą, atitinkančią Europos Sąjungos pagrindinių teisių chartijos (toliau – **Chartija**) 47 straipsnio reikalavimus, t. y. kuri yra kompetentinga nustatyti, kad duomenys yra tvarkomi, patikrinti tvarkymo teisėtumą ir kuri turi vykdytinus taisomuosius įgaliojimus tuo atveju, jei duomenų tvarkymas yra neteisėtas. Šiomis aplinkybėmis EDAV prašo Europos Komisijos patikslinti, ar PIPC pateiktam skundui arba bet kokiam ieškiniui teisme taikomi esminiai ir (arba) procedūriniai reikalavimai, pavyzdžiui, prievolė įrodyti, ir ar asmenys EEE galėtų įvykdyti tokią išankstinę sąlygą.

1.3. Išvada

24. EDAV mano, kad šis sprendimas dėl tinkamumo yra nepaprastai svarbus, taip pat atsižvelgiant į tai, kad – išskyrus nuomonėje nurodytas išimtis – jis apims duomenų perdavimą ir viešajame, ir privačiajame sektoriuose.

25. EDAV palankiai vertina Europos Komisijos ir Korėjos institucijų pastangas suderinti Korėjos teisinę sistemą su Europos teisine sistema. Patobulinimai, kuriuos ketinama padaryti Pranešimu Nr. 2021-1 ir kuriais siekiama panaikinti kai kuriuos šių dviejų sistemų skirtumus, yra labai svarbūs ir vertinami palankiai. Tačiau EDAV atkreipia dėmesį į tai, kad vis dar išlieka daug susirūpinimą keliančių klausimų, įskaitant susijusius su Pranešimu Nr. 2021-1, kartu su poreikiu labiau patikslinti kitus klausimus, ir

rekomenduoja Europos Komisijai reaguoti į EDAV iškeltus rūpimus klausimus ir patikslinimo prašymus bei pateikti daugiau informacijos ir paaiškinimų dėl šioje nuomonėje iškeltų klausimų.

2. ĮVADAS

2.1. Korėjos duomenų apsaugos sistema

26. Pagrindinis teisės aktas, reglamentuojantis duomenų apsaugą Korėjos Respublikoje, yra Asmens duomenų apsaugos įstatymas (2011 m. kovo 29 d. įstatymas Nr. 10465, paskutinį kartą pakeistas 2020 m. vasario 4 d. įstatymu Nr. 16930 (toliau – **PIPA**). Jis papildytas vykdymo dekretu (2011 m. rugsėjo 29 d. Prezidento dekretas Nr. 23169, paskutinį kartą pakeistas 2020 m. rugpjūčio 4 d. Prezidento dekretu Nr. 30892, toliau – PIPA vykdymo dekretas), kuris yra teisiškai privalomas ir vykdytinas.

27. Be PIPA, Korėjos duomenų apsaugos sistemoje yra Korėjos priežiūros institucijos – Asmens duomenų apsaugos komisijos (toliau – **PIPC**) – pateikti reglamentavimo pranešimai, kuriuose pateikiamos papildomos PIPA aiškinimo ir taikymo taisyklės. Neseniai PIPC priėmė 2021 m. sausio 21 d. Pranešimą Nr. 2021-1 (kuriuo iš dalies pakeistas ankstesnis 2020 m. rugsėjo 1 d. Pranešimas Nr. 2020-10, toliau – **Pranešimas Nr. 2021-1**) dėl tam tikrų PIPA nuostatų aiškinimo, taikymo ir vykdymo. Tiksliau, šis pranešimas parengtas po Korėjos institucijų ir Europos Komisijos diskusijų dėl tinkamumo. Jame pateikiami paaiškinimai, kaip taikyti konkrečias PIPA nuostatas, įskaitant asmens duomenų, perduotų Korėjai remiantis numatomu sprendimu dėl tinkamumo[8], tvarkymą ir jis *turi administracinės taisyklės, turinčios teisiškai privalomą galią asmens duomenų valdytojui, statusą, nes bet koks pranešimo pažeidimas gali būti laikomas atitinkamų PIPA nuostatų pažeidimu*[9]. Atsižvelgdama į tai, EDAV norėtų pažymėti, kad, nepaisant to, jog sprendimo projekte pranešimas vadinamas papildomomis taisyklėmis, į jį neįtrauktos papildomos taisyklės *per se*, o veikiau paaiškinimai, kuriais siekiama patikslinti, kaip turėtų būti suprantamas įstatymu nustatytas PIPA tekstas, kad būtų galima jį taikyti, visų pirma iš EEE perduotų duomenų atžvilgiu. Šiomis aplinkybėmis EDAV rekomenduotų atidžiai stebėti, kaip praktiškai laikomasi Pranešimo Nr. 2021-1, visų pirma atsižvelgiant į tai, kaip jį taiko ne tik PIPC, bet ir teismai, ypač kai lygiavertis apsaugos lygis, kurį užtikrina Korėjos teisinė sistema, yra grindžiamas Pranešime Nr. 2021-1 pateiktais paaiškinimais.

28. Kitais susijusiais Korėjos teisės aktų sistemos duomenų apsaugos įstatymais nustatomos asmens duomenų tvarkymo taisyklės tam tikruose pramonės sektoriuose, pavyzdžiui:

- Kredito informacijos naudojimo ir apsaugos įstatymas (toliau – **CIA**), įskaitant jo vykdymo dekretą (toliau – **CIA vykdymo dekretas**), kuriame nustatomos konkrečios taisyklės, taikomos komercinės veiklos vykdytojams ir specializuotiems subjektams (pvz., kredito reitingų agentūroms, finansų įstaigoms) kai jie tvarko asmeninę kredito informaciją, būtiną finansinių ar komercinių sandorių šalių kreditingumui nustatyti;

- Informacijos ir ryšių tinklų naudojimo ir duomenų apsaugos skatinimo įstatymas (toliau – **Tinklų įstatymas**), ir

- Ryšių privatumo apsaugos įstatymas (toliau – **CPPA**).

29. Kalbant apie vyriausybės prieigą, be atitinkamų PIPA ir CPPA nuostatų, EDAV apsvarstė kai kuriuos kitus teisės aktus, t. y. Baudžiamojo proceso įstatymą (toliau – **CPA**), Telekomunikacijų verslo įstatymą (toliau – **TBA**), Įstatymą dėl ataskaitų teikimo ir nurodytų finansinių sandorių informacijos naudojimo (toliau – **ARUSFTI**) ir Nacionalinės žvalgybos tarnybos įstatymą (toliau – **NISA**).

[8] Žr. sprendimo projekto I priedo I skyrių.
[9] Ten pat.

2.2. EDAV vertinimo apimtis

30. Europos Komisijos sprendimo projektas yra Korėjos duomenų apsaugos sistemos įvertinimo, po kurio vyko diskusijos su Korėjos vyriausybe, rezultatas. EDAV pagal BDAR 70 straipsnio 1 dalies s punktą turėtų pateikti nepriklausomą nuomonę apie Europos Komisijos išvadas, nustatyti tinkamumo sistemos trūkumus (jei jų yra) ir stengtis pateikti pasiūlymų jiems ištaisyti.

31. Siekdama išvengti pasikartojimo ir padėti įvertinti Korėjos teisinę sistemą, EDAV nusprendė sutelkti dėmesį į kai kuriuos konkrečius sprendimo projekte pateiktus punktus ir pateikti jų analizę bei nuomonę apie juos, susilaikydama nuo daugumos faktinių išvadų ir vertinimų pakartojimo, kai EDAV neturi pagrindo manyti, kad Korėjos Respublikos teisė iš esmės nebūtų lygiavertė EEE teisei. Be to, atsižvelgiant į ESTT praktiką, labai svarbi analizės dalis apima teisinę tvarką, pagal kurią nacionalinio saugumo institucijos turi prieigą prie Korėjos Respublikai perduotų asmens duomenų, ir jos nacionalinio saugumo aparato veiklą.

32. Savo vertinime EDAV atsižvelgė į taikomą Europos duomenų apsaugos sistemą, įskaitant Chartijos 7, 8 ir 47 straipsnius, atitinkamai ginančius teisę į privatų ir šeimos gyvenimą, teisę į asmens duomenų apsaugą ir teisę į veiksmingus taisomuosius veiksmus ir teisingą bylos nagrinėjimą, ir į Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (EŽTK) 8 straipsnį, ginantį teisę į privatų ir šeimos gyvenimą. Be to, kas išdėstyta pirmiau, EDAV apsvarstė BDAR reikalavimus ir atitinkamą teismų praktiką.

33. Šio tyrimo tikslas – pateikti Europos Komisijai nuomonę dėl Korėjos Respublikos apsaugos lygio tinkamumo įvertinimo. ESTT toliau formavo sąvoką „tinkamas apsaugos lygis“, kuri jau buvo numatyta Direktyvoje 95/46. Svarbu prisiminti ESTT sprendime *Schrems I* nustatytą standartą, t. y. kad, nors „apsaugos lygis“ trečiojoje šalyje turi būti „iš esmės lygiavertis“ ES užtikrinamam lygiui, „*priemonės, kurių ši trečioji šalis šiuo klausimu imasi siekdama užtikrinti tokį apsaugos lygį, gali skirtis nuo priemonių [ES]*“[10]. Todėl tikslas yra ne papunkčiui atspindėti Europos teisės aktus, o nustatyti esminius ir pagrindinius nagrinėjamų teisės aktų reikalavimus. Tinkamumą gali užtikrinti duomenų subjektų teisių ir duomenis tvarkančių subjektų arba nepriklausomų institucijų, kurios kontroliuoja šį tvarkymą, pareigų derinys. Vis dėlto duomenų apsaugos taisyklės yra veiksmingos tik tada, kai jos įgyvendinamos ir jų laikomasi praktiškai. Todėl būtina atsižvelgti ne tik į taisyklių, taikomų trečiajai šaliai arba tarptautinei organizacijai perduodamiems asmens duomenims, turinį, bet ir į nustatytą sistemą, taikomą siekiant užtikrinti tokių taisyklių veiksmingumą. Veiksmingi vykdymo užtikrinimo mechanizmai yra ypač svarbūs siekiant duomenų apsaugos taisyklių veiksmingumo[11].

2.3. Bendrosios pastabos ir susirūpinimą keliantys klausimai

2.3.1. Korėjos Respublikos prisiimti tarptautiniai įsipareigojimai

34. Pagal BDAR 45 straipsnio 2 dalies c punktą ir BDAR darbinį dokumentą dėl referencinio tinkamumo[12] Europos Komisija, vertindama trečiosios šalies apsaugos lygio tinkamumą, be kita ko, atsižvelgia į tarptautinius įsipareigojimus, kuriuos prisiėmė trečioji šalis, arba kitus įsipareigojimus, kurie atsiranda dėl trečiosios šalies dalyvavimo daugiašalėse ar regioninėse sistemose, visų pirma susijusiose su asmens duomenų apsauga, taip pat į tokių prievolių įgyvendinimą.

35. Korėja yra kelių tarptautinių susitarimų, garantuojančių teisę į privatumą, pavyzdžiui, Tarptautinio pilietinių ir politinių teisių pakto (17 straipsnis), Neįgaliųjų teisių konvencijos (22 straipsnis) ir Vaiko

[10] 2015 m. spalio 6 d. Teisingumo Teismo sprendimas *Maximilian Schrems prieš Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650, 73 ir 74 punktai.
[11] WP254, p. 2.
[12] WP254, p. 2.

teisių konvencijos (16 straipsnis), šalis. Be to, Korėja, kaip EBPO narė, laikosi EBPO privatumo sistemos, visų pirma gairių, reglamentuojančių privatumo ir tarpvalstybinių asmens duomenų srautų apsaugą.

36. EDAV taip pat atkreipia dėmesį į Korėjos, kaip valstybės stebėtojos, dalyvavimą Europos Tarybos konvencijos Nr. 108 (+) Konsultacinio komiteto darbe, nors ji dar nenusprendė, ar prie jos prisijungti.

2.3.2. Sprendimo dėl tinkamumo taikymo sritis.

37. Remiantis sprendimo projekto 5 konstatuojamąja dalimi, Europos Komisija daro išvadą, kad Korėjos Respublika užtikrina tinkamą asmens duomenų, perduodamų iš Sąjungoje esančio duomenų valdytojo ar tvarkytojo asmens duomenų valdytojams (pvz., fiziniams ar juridiniams asmenims, organizacijoms, valstybės institucijoms), patenkantiems į PIPA taikymo sritį, išskyrus religinių organizacijų asmens duomenų tvarkymą misionieriškai veiklai vykdyti ir politinių partijų kandidatų siūlymui užtikrinti[13], arba asmeninės kredito informacijos tvarkymą pagal CIA, kurį atlieka Finansinių paslaugų komisijos prižiūrimi valdytojai.

38. EDAV pažymi, kad sprendimas dėl tinkamumo apims duomenų perdavimą iš EEE teisinės sistemos tiek viešiesiems, tiek privatiesiems asmens duomenų valdytojams, kuriems taikomas PIPA. EDAV supranta, kad subjektams, veikiantiems kaip duomenų tvarkytojai, kaip apibrėžta BDAR, taip pat taikoma sąvoka „asmens duomenų valdytojas“, atsižvelgiant į tai, kad PIPA jiems bus taikoma vienodai, o kai asmens duomenų valdytojas („užsakovas“) pasitelkia trečiąją šalį asmens duomenims tvarkyti („užsakomasis subjektas“), taikomi specialūs įpareigojimai, tačiau, siekiant išvengti nesusipratimų, EDAV ragina Europos Komisiją patikslinti, kad sprendimas dėl tinkamumo taip pat apims duomenų perdavimą „tvarkytojams“ Korėjoje ir kad tais atvejais taip pat nebus pakenkta iš EEE perduotų asmens duomenų apsaugos lygiui.

39. Be to, atsižvelgiant į tai, kad sprendimas dėl tinkamumo taip pat apima asmens duomenų perdavimą tarp viešųjų įstaigų, EDAV supranta, kad į tai taip pat įeina duomenų perdavimas tarp duomenų apsaugos priežiūros institucijų ir, siekdama aiškumo, ragina Europos Komisiją konkrečiai spręsti šį klausimą.

40. Be to, subjektų, kuriems netaikomas sprendimas dėl tinkamumo, atžvilgiu EDAV norėtų pabrėžti, kad kalbant apie sprendimą dėl tinkamumo galėtų būti naudinga, jei būtų aiškiau nustatytos komercinės organizacijos, kurioms taikoma PIPC priežiūra (CIA 45 straipsnio 3 dalis), kad EEE duomenų valdytojai ir tvarkytojai prieš perduodami duomenis subjektams, kuriems taikomas CIA, galėtų lengvai įvertinti, ar importuotojas taip pat patenka į sprendimo dėl tinkamumo taikymo sritį, arba bent jau būti įspėti, kad reikia įvertinti šį aspektą.

41. Kalbant apie sprendimo dėl tinkamumo taikymo sritį, EDAV iš papildomų Europos Komisijos paaiškinimų suprato, kad Korėjos finansinės žvalgybos padalinys (toliau – **KOFIU**), kuris yra įsteigtas prie Finansinių paslaugų komisijos ir rūpinasi pinigų plovimo ir teroristų finansavimo prevencija pagal ARUSFTI[14], taip pat nėra įtrauktas į taikymo sritį, nes jis turi kompetenciją tik finansų įstaigų, kurių pačių neapima sprendimo projektas, atžvilgiu. Tačiau į sprendimo projekto 1 straipsnio 2 dalies c punkto taikymo sritį neįtraukti tik tie asmens duomenų valdytojai, kuriuos prižiūri Finansinių paslaugų komisija ir kurie tvarko asmeninę kredito informaciją pagal CIA. Atsižvelgdama į tai, EDAV prašo Europos Komisijos paaiškinti, ar KOFIU ir pati KOFIU vykdoma duomenų tvarkymo veikla patenka į sprendimo projekto taikymo sritį.

[13] Daugiau informacijos rasite toliau šios nuomonės 3.1.2 skyriuje.
[14] Žr. II priedo 2.2.3.1 skyrių.

3. BENDRIEJI DUOMENŲ APSAUGOS ASPEKTAI

3.1. Turinio principai

42. BDAR darbinio dokumento dėl referencinio tinkamumo 3 skyrius skirtas turinio principams. Jie turi būti įtraukti į trečiosios šalies sistemą, siekiant užtikrinti, kad teikiamos apsaugos lygis iš esmės būtų lygiavertis tam, kurį garantuoja ES teisės aktai.

43. Nors teisė į asmens duomenų apsaugą nėra aiškiai įtvirtinta Korėjos konstitucijoje *per se*, ji pripažįstama kaip pagrindinė teisė, kylanti iš konstitucinių teisių į žmogaus orumą ir laimės siekimą (10 straipsnis), privatų gyvenimą (17 straipsnis) ir ryšių privatumą (18 straipsnis). Tai patvirtino ir Aukščiausiasis Teismas, ir Konstitucinis Teismas, kaip nurodyta Europos Komisijos sprendimo projekte[15]. EDAV atkreipia dėmesį į šį pripažinimą, nes iš jo galima daryti išvadą, kad duomenų apsauga, kaip pagrindinė teisė, pagal Korėjos Konstitucijos 37 straipsnį *„gali būti apribota tik įstatymu ir kai tai būtina nacionaliniam saugumui arba teisėtvarkai palaikyti ar visuomenės gerovei užtikrinti*" ir kad *„net jei tokie apribojimai yra nustatyti, jie negali turėti įtakos laisvės ar teisės esmei"*.

44. Europos Komisijos teigimu[16], Konstitucinis Teismas nusprendė, kad ir užsienio piliečiai yra pagrindinių teisių subjektas. Remiantis oficialiais Korėjos vyriausybės pareiškimais[17], nors teismų praktikoje iki šiol nebuvo konkrečiai nagrinėjama ne Korėjos piliečių teisė į privatumą, tarp mokslininkų plačiai pripažįstama, kad Konstitucijos 12–22 straipsniuose yra nustatytos „žmogaus teisės". Be to, Korėjos Respublika priėmė daugybę duomenų apsaugos srities įstatymų, pavyzdžiui, PIPA, pagal kuriuos suteikiama apsauga visiems asmenims nepriklausomai nuo jų pilietybės. Šiuo atžvilgiu EDAV atkreipia dėmesį į tai, kad Konstitucijos 6 straipsnio 2 dalyje nustatyta, jog užsienio piliečių statusas yra garantuojamas taip, kaip nurodoma tarptautinėje teisėje ir sutartyse bei sprendimo projekte minimoje teismų praktikoje, pagal kurią „užsienietis" gali būti „pagrindinių teisių" turėtojas. Atsižvelgdama į užsienio piliečių teisės į duomenų apsaugą pripažinimo svarbą, EDAV ragina Europos Komisiją atkreipti dėmesį į būtinybę ir toliau stebėti teismų praktiką, susijusią su duomenų apsauga, kaip pagrindine teise, kuri pripažįstama ne tik kaip Korėjos piliečių, bet visų duomenų subjektų teisė, siekiant užtikrinti, kad BDAR garantuojamam fizinių asmenų apsaugos lygiui nebūtų pakenkta, kai asmens duomenys pagal sprendimą dėl tinkamumo perduodami Korėjai.

3.1.1. Sąvokos

45. Pagal BDAR darbinį dokumentą dėl referencinio tinkamumo, trečiosios šalies teisinėje sistemoje turėtų būti įtvirtintos pagrindinės duomenų apsaugos sąvokos ir (arba) principai. Nors jie ir neturi sutapti su BDAR terminija, juose turėtų atsispindėti Europos duomenų apsaugos teisėje įtvirtintos sąvokos ir jie turi jas atitikti. Pavyzdžiui, į BDAR įtrauktos šios svarbios sąvokos: „asmens duomenys", „asmens duomenų tvarkymas", „duomenų valdytojas", „duomenų tvarkytojas", „gavėjas" ir „neskelbtini duomenys"[18].

46. PIPA apima daug apibrėžčių, pvz., be kita ko, „asmens duomenų", „tvarkymo" ir „duomenų subjekto", kurios labai panašios į atitinkamas BDAR sąvokas.

3.1.1.1. Pseudoniminių duomenų sąvoka

47. Tarp PIPA pateiktų apibrėžčių, visų pirma PIPA 2 straipsnio 1 dalyje, asmens duomenys apibrėžiami kaip bet kurie iš toliau nurodytų su gyvu asmeniu susijusių duomenų: a) duomenys, iš kurių

[15] Žr. sprendimo projekto 8 konstatuojamąją dalį ir atitinkamą teismų praktiką, nurodytą sprendimo projekto 10 išnašoje, kurioje pateikiamos tik santraukos anglų kalba.
[16] Žr. sprendimo projekto 9 konstatuojamąją dalį.
[17] Sprendimo projekto II priedo 1.1. skyrius.
[18] WP254, p. 4.

nustatomas konkretus asmuo pagal jo vardą, pavardę, gyventojo registracijos numerį, atvaizdą ir pan., ir b) duomenys, kurie, net jei pagal juos pačius nenustatomas konkretus asmuo, gali būti lengvai derinami su kitais duomenimis, kad būtų galima nustatyti konkretų asmenį. Pastaruoju atveju tai, ar lengva informaciją derinti, ar ne, nustatoma pagrįstai įvertinant laiką, sąnaudas, technologijas ir pan., naudojamus asmeniui nustatyti, taip pat tikimybę, kad bus galima gauti kitos informacijos.

48. Be to, pagal PIPA 2 straipsnio 1 dalies c punktą, pseudoniminiai duomenys taip pat yra laikomi asmens duomenimis. Pseudoniminė informacija apibrėžiama kaip pirmiau minėto straipsnio 1 dalies a arba b punktuose nurodyta informacija, kuriai suteikti pseudonimai pagal 1 ir 2 dalis ir dėl to pagal ją nebejmanoma nustatyti konkretaus asmens, nenaudojant kitos informacijos ar nederinant informacijos, kad būtų atkurta pradinė būsena. Informacija, kuri yra visiškai anonimiška, neįtraukiama į PIPA taikymo sritį. Pagal PIPA 58 straipsnio 2 dalį šis įstatymas netaikomas informacijai, pagal kurią nebegalima nustatyti tam tikro asmens, kai ji derinama su kita informacija, pagrįstai atsižvelgiant į laiką, sąnaudas, technologijas ir kt.

49. Europos Komisija savo sprendimo projekto 17 konstatuojamojoje dalyje teigia, kad tai atitinka materialinę BDAR taikymo sritį ir jos sąvokas „asmens duomenys“, „pseudonimų suteikimas“ ir „anonimizuota informacija“.

50. Tačiau pagal PIPA 28 straipsnio 7 dalį, 20, 21, 27 straipsniai, 34 straipsnio 1 dalis, 35–37 straipsniai, 39 straipsnio 3 ir 4 dalys, 39 straipsnio 6–8 dalys netaikomos pseudoniminiams asmens duomenims.

51. Europos Komisija savo sprendimo projekte nurodo, kad PIPA 28 straipsnio 7 dalis taikoma tik pseudoniminiams asmens duomenims, kai jie yra tvarkomi statistikos, mokslinių tyrimų ar archyvavimo tikslais dėl viešojo intereso[19]. Tačiau tai išdėstyta įstatyme, o Pranešime Nr. 2021-1 pateiktuose paaiškinimuose[20]. Nors EDAV pripažįsta, kad remiantis PIPA struktūra ir loginiu pagrindu galima pateikti argumentą, kad PIPA 28 straipsnio 2 dalis turėtų būti suprantama ir logiškai aiškinama taip, kad ji taip pat taikoma PIPA 28 straipsnio 7 daliai, atsižvelgiant į Pranešimo Nr. 2021-1 svarbą Europos Komisijos atliktame asmens duomenų apsaugos lygio tinkamumo Korėjos Respublikoje vertinime ir, kad būtų išvengta bet kokių abejonių, EDAV ragina Europos Komisiją pateikti papildomos informacijos apie Pranešimo Nr. 2021-1 privalomumą, įgyvendinamumą ir galiojimą bei stebėti jo taikymą šiomis konkrečiomis aplinkybėmis.

52. Atsižvelgdama į tai, EDAV norėtų priminti, kad pagal BDAR pseudoniminimas yra suprantamas kaip rekomenduojama saugumo priemonė. Kitaip tariant, pagal BDAR pseudoniminiai duomenys išlieka asmens duomenimis, kuriems visapusiškai taikomas BDAR. Remiantis tuo, kas išdėstyta pirmiau, EDAV nerimauja, kad BDAR pseudoniminių asmens duomenų apsaugos lygis gali būti sumažintas, kai asmens duomenys perduodami Korėjai. Todėl EDAV prašo Europos Komisijos toliau vertinti pseudonimų suteikimo poveikį pagal PIPA ir, svarbiausia, kaip tai gali paveikti duomenų subjektų, kurių asmens duomenys būtų perduodami Korėjos Respublikai pagal sprendimą dėl tinkamumo, pagrindines teises ir laisves. Todėl EDAV ragina Europos Komisiją užtikrinti, kad EEE duomenų subjektų asmens duomenų apsaugos lygis nebūtų sumažintas po perdavimo Korėjos Respublikai, net jei perduodami asmens duomenys yra pseudoniminiai.

3.1.1.2. *Asmens duomenų valdytojo sąvoka*

53. Į PIPA 2 straipsnio 5 dalį įtraukta „asmens duomenų valdytojo“ apibrėžtis, reiškianti viešąją instituciją, juridinį asmenį, organizaciją ar asmenį ir pan., kuris tiesiogiai ar netiesiogiai tvarko asmens duomenis, kad galėtų tvarkyti asmens duomenų bylas „*kaip savo veiklos dalį*“. Tačiau papildomose apsaugos

[19] Žr., *inter alia*, sprendimo projekto 82 konstatuojamąją dalį.
[20] Sprendimo projekto I priedo 4 skyrius.

priemonėse, nustatytose Pranešime Nr. 2021-1, asmens duomenų valdytojo sąvoka apibrėžiama kaip viešoji institucija, juridinis asmuo, organizacija, fizinis asmuo ir pan., kuris tiesiogiai ar netiesiogiai tvarko asmens duomenis, kad galėtų tvarkyti asmens duomenų bylas „*verslo tikslais*“. Tuo tarpu sprendimo projekto 272 išnašoje apie asmens duomenų valdytojo sąvoką nurodyta: „*Kaip apibrėžta PIPA 2 straipsnyje, t. y. viešoji institucija, juridinis asmuo, organizacija, fizinis asmuo ir pan., kuris tiesiogiai ar netiesiogiai tvarko asmens duomenis, kad galėtų tvarkyti asmens duomenų bylas „oficialiais ar verslo tikslais*“.

54. EDAV pripažįsta, kad šie neatitikimai gali atsirasti dėl Korėjos valdžios institucijų pateikto teksto originalo kalba vertimų, ir prašo Europos Komisijos reguliariai tikrinti vertimų kokybę ir tikslumą. Tačiau EDAV pabrėžia, kad, norint įvertinti esminį Korėjos teisinės sistemos duomenų apsaugos lygio lygiavertiškumą, reikia aiškiai suprasti duomenų tvarkymo tikslus, kurie patenka į PIPA materialinę taikymo sritį. Be to, šiomis aplinkybėmis EDAV pažymi, kad PIPA nėra naudojama tokia pati kaip BDAR terminija, susijusi su „valdytojo“ ir „tvarkytojo“ sąvokomis, ir ragina Europos Komisiją patikslinti teisingą sąvokos „asmens duomenų valdytojas“ apibrėžtį bei taikymo sritį ir konkrečiai spręsti, ar šis terminas taip pat apima duomenų tvarkytojus, kaip apibrėžta BDAR, nes tai daro tiesioginį poveikį sprendimo dėl tinkamumo taikymo sričiai[21].

3.1.2. PIPA nustatytos dalinės išimtys

55. PIPA 58 straipsnio 1 dalyje nustatyta, kad tam tikros PIPA dalys (t. y. 15–57 straipsniai) netaikomi keturių kategorijų asmens duomenų tvarkymui, kaip aprašyta toliau. Konkrečiai, išimtys susijusios su PIPA nuostatomis dėl konkrečių tvarkymo pagrindų, tam tikrų duomenų apsaugos įpareigojimų, išsamių taisyklių dėl naudojimosi asmens teisėmis, taip pat ginčų sprendimą reglamentuojančių taisyklių. Tačiau EDAV atkreipia dėmesį į tai, kad vis dar taikomos kai kurios bendros PIPA nuostatos, pavyzdžiui, susijusios su duomenų apsaugos principais (PIPA 3 straipsnis) ir individualiomis teisėmis (PIPA 4 straipsnis). Be to, PIPA 58 straipsnio 4 dalyje nustatyti konkretūs įpareigojimai šioms keturioms duomenų tvarkymo kategorijoms.

56. Pirma, dalinė išimtis taikoma asmens duomenims, surinktiems pagal Statistikos įstatymą, kad juos tvarkytų viešosios institucijos. Europos Komisija savo sprendimo projekto 27 konstatuojamojoje dalyje nurodo, kad, remiantis Korėjos vyriausybės pateiktais paaiškinimais, šiomis aplinkybėmis tvarkomi asmens duomenys paprastai yra susiję su Korėjos piliečiais ir tik išimties tvarka gali apimti informaciją apie užsieniečius, būtent statistiką apie įvažiavimą į teritoriją ir išvykimą iš jos, arba apie užsienio investicijas. Tačiau, remiantis sprendimo projektu, net ir tokiose situacijose šie duomenys paprastai nėra perduodami iš EEE duomenų valdytojų ir (arba) duomenų tvarkytojų, o veikiau juos tiesiogiai renka Korėjos valdžios institucijos.

57. EDAV pripažįsta Europos Komisijos argumentus dėl išimtinio Statistikos įstatymo taikymo pobūdžio tvarkant pagal sprendimą dėl tinkamumo perduotus asmens duomenis, tačiau norėtų gauti papildomos informacijos ir patikinimų apie konkrečias apsaugos priemones, kurios būtų taikomos tuo atveju, jei iš EEE perduoti asmens duomenys bus toliau renkami pagal Statistikos įstatymą, kad juos tvarkytų viešosios institucijos, visų pirma susiję su duomenų subjektų naudojimusi individualiomis teisėmis pagal BDAR 89 straipsnio 2 dalį, tiek, kiek tikėtina, kad dėl tokių teisių nebus neįmanoma pasiekti konkrečių tikslų arba jos netrukdys juos pasiekti, ir tokios nukrypti leidžiančios nuostatos nėra būtinos šiems tikslams įgyvendinti.

58. Atsižvelgiant į tai, atrodo, kad PIPA 4 straipsnio taikymas taip pat ir tokiam duomenų tvarkymui išsklaido susirūpinimą, tačiau EDAV norėtų, kad sprendime dėl tinkamumo būtų pateikta papildomos informacijos ir paaiškinimų apie konkrečius įpareigojimus, pagal PIPA 58 straipsnio 4 dalį nustatytus

[21] Taip pat žr. pirmiau pateiktą 38 punktą.

šiai tvarkymo veiklai, būtent dėl duomenų kiekio mažinimo, riboto duomenų saugojimo, saugumo priemonių ir skundų nagrinėjimo.

59. Antra, dalinė išimtis taikoma asmens duomenims, kurie surinkti arba yra prašoma juos pateikti su nacionaliniu saugumu susijusios informacijos analizei atlikti. EDAV žino, kad nacionalinio saugumo klausimais valstybės turi plačią, EŽTT pripažintą veiksmų laisvę. EDAV taip pat pažymi, kad pagal Korėjos Konstitucijos 37 straipsnio 2 dalį bet koks laisvių ir teisių apribojimas, pavyzdžiui, kai tai būtina siekiant užtikrinti nacionalinį saugumą, negali pažeisti esminio tos laisvės ar teisės aspekto. Be to, EDAV atkreipia dėmesį į Pranešimo Nr. 2021-1 6 skyriuje pateiktas apsaugos priemones, susijusias su asmens duomenų tvarkymu nacionalinio saugumo tikslais, įskaitant pažeidimų tyrimą ir sprendimų vykdymą. Tačiau šiomis aplinkybėmis EDAV ragina Europos Komisiją labiau patikslinti išimčių taikymo sritį, nes jai kyla klausimas, ar visos išimtys, numatytos PIPA 58 straipsnio 1 dalies 2 punkte (III–VII skyriai), yra svarbios žvalgybos tarnybų darbui ir ar jos užtikrina lygiavertiškumą būtinumo ir proporcingumo principams. Visų pirma EDAV ragina Europos Komisiją labiau patikslinti, kokiomis aplinkybėmis žvalgybos tarnyba galėtų remtis išimtimis. EDAV mano, kad būtina atidžiai stebėti šių apribojimų poveikį praktikoje, ypač efektyviam duomenų subjektų naudojimuisi savo teisėmis ir jų įgyvendinimui.

60. Trečia, dalinė išimtis taikoma *„asmens duomenims, kuri laikinai tvarkoma, kai tai skubiai būtina visuomenės saugai ir saugumui, visuomenės sveikatai ir pan.“*. Remiantis Europos Komisijos sprendimo projekto 29 konstatuojamąja dalimi; PIPC griežtai aiškina šią kategoriją ir ši išimtis taikoma tik ekstremaliųjų situacijų atvejais, kai reikia skubių veiksmų, pavyzdžiui, siekiant nustatyti infekcijos sukėlėjus arba gelbėti nukentėjusiuosius nuo stichinių nelaimių ir jiems padėti.

61. EDAV taip pat pabrėžia, kad bet kokios nukrypti nuo asmens duomenų apsaugos lygio leidžiančios nuostatos turėtų būti aiškinamos griežtai. Tuo pat metu EDAV pažymi, kad ši nuostata nėra griežtai apibrėžta ir nepateikiamas išsamus situacijų, kai asmens duomenų tvarkymas gali būti laikomas „*skubiai būtinu*“, pavyzdžių sąrašas. Pavyzdžiui, EDAV yra susirūpinusi, ar tarptautinis sveikatos duomenų perdavimas besitęsiančios COVID-19 pandemijos metu taip pat patektų į šios išimties taikymo sritį. Atsižvelgdama į tai, kas išdėstyta pirmiau, EDAV ragina Europos Komisiją labiau patikslinti šios išimties taikymo sritį ir visapusiškai stebėti jos taikymą ir taikymo sritį, siekiant užtikrinti, kad dėl to nebūtų sumažintas EEE asmens duomenų apsaugos lygis po jų perdavimo Korėjai pagal sprendimą dėl tinkamumo.

62. Galiausiai, dalinė išimtis taikoma asmens duomenims, surinktiems ar naudojamiems spaudos pranešimams rengti, religinių organizacijų misionieriškai veiklai vykdyti ir politinių partijų kandidatų siūlymui užtikrinti[22]. Kalbant apie asmens duomenų tvarkymą, kurį atlieka spauda žurnalistinei veiklai vykdyti, Europos Komisija savo sprendimo projekto 31 konstatuojamojoje dalyje nurodo, kad žodžio laisvės ir kitų teisių, įskaitant teisę į privatumą, pusiausvyros užtikrinimas numatytas Įstatyme dėl arbitražo ir taisomųjų veiksmų ir kt. dėl žalos, padarytos pranešimais spaudai (toliau – **Spaudos įstatymas**), ir pateikia Spaudos įstatyme numatytas konkrečias apsaugos priemones. Tačiau EDAV ragintų Europos Komisiją visapusiškai stebėti šią išimtį ir atitinkamą teismų praktiką, siekiant užtikrinti, kad lygiavertis duomenų apsaugos lygis Korėjos teisinėje sistemoje būtų užtikrintas ir praktiškai.

3.1.3. Teisėto ir sąžiningo duomenų tvarkymo teisėtais tikslais pagrindai

63. Pagal BDAR darbinį dokumentą dėl referencinio tinkamumo, remiantis BDAR duomenys turi būti tvarkomi teisėtai, sąžiningai ir pagrįstai. Turėtų būti pakankamai aiškiai nustatytas teisinis pagrindas, kuriuo remiantis asmens duomenys gali būti teisėtai, sąžiningai ir pagrįstai tvarkomi. Europos sistemoje pripažįstami keli tokie teisėti pagrindai, įskaitant, pavyzdžiui, nacionalinės teisės nuostatas,

[22] Atitinkamai, į sprendimo dėl tinkamumo taikymo sritį taip pat neįtrauktas religinių organizacijų atliekamas asmens duomenų tvarkymas savo misionieriškai veiklai vykdyti ir politinių partijų atliekamas asmens duomenų tvarkymas siūlant kandidatus. Taip pat žr. pirmiau pateiktą 2.3.2 skyriaus 37 punktą.

duomenų subjekto sutikimą, sutarties vykdymą arba duomenų valdytojo ar trečiosios šalies teisėtus interesus, kurie nėra viršesni už asmens interesus.

64. Laikantis panašios struktūros kaip BDAR, pagal PIPA pradžioje apibrėžiamas teisėtumo, sąžiningumo ir skaidrumo principas (PIPA 3 straipsnio 1 ir 2 dalys), vėliau nustatant konkrečias jo taikymo taisykles (PIPA 15–19 straipsniai). Konkrečiai, PIPA 15 straipsnis apima teisinių pagrindų katalogą, kuriuo asmens duomenų valdytojai gali remtis rinkdami asmens duomenis ir naudoti juos pagal rinkimo tikslą. Šie teisiniai pagrindai yra: 1) informacija grindžiamas duomenų subjekto sutikimas; 2) įstatymu nustatytas leidimas arba būtinybė laikytis teisinio įpareigojimo; 3) būtinybė vykdyti viešosios institucijos pareigas; 4) sutarties su duomenų subjektu vykdymo būtinybė; 5) būtinybė apsaugoti duomenų subjekto ar trečiosios šalies gyvybę, kūno ar turtinius interesus nuo neišvengiamo pavojaus (ir nėra galimybės gauti išankstinio sutikimo); 6) būtinybė tenkinti pagrįstą asmens duomenų valdytojo interesą, pranašesnį už duomenų subjekto interesą.

65. Be to, PIPA 17 straipsnyje išvardyti teisiniai pagrindai, taikomi dalijimuisi asmens duomenimis su trečiąja šalimi, yra šie: 1) informacija grindžiamas duomenų subjekto sutikimas; 2) įstatymu nustatytas leidimas arba būtinybė laikytis teisinio įpareigojimo; 3) būtinybė vykdyti viešosios institucijos pareigas; ir 4) būtinybė apsaugoti duomenų subjekto ar trečiosios šalies gyvybę, kūno ar turtinius interesus nuo neišvengiamo pavojaus (ir nėra galimybės gauti išankstinio sutikimo). Net ir nesant duomenų subjekto sutikimo, dalytis asmens duomenimis leidžiama, kai tai įvyksta ribose, pagrįstai susijusiose su tikslais, kuriais iš pradžių buvo renkami asmens duomenys (PIPA 17 straipsnio 4 dalis).

66. PIPA 18 straipsnyje nustatytos specialios asmens duomenų naudojimo ir dalijimosi jais taisyklės, kai tai neatitinka pirminio informacijos rinkimo ar teikimo tikslo. Be kita ko, ir šiuo atveju sutikimas yra viena iš tokių leidžiančių taisyklių.

67. Pripažindama esminį Korėjos teisės panašumą į BDAR, atsižvelgiant į teisėtumo principą ir bendrąją teisę į duomenų tvarkymo sustabdymą (PIPA 37 straipsnis), kuria taip pat galima remtis, kai asmens duomenys tvarkomi sutikimo pagrindu, EDAV norėtų pažymėti, kad pagal PIPA nėra nustatytos bendros teisės atšaukti sutikimą[23]. Atsižvelgdama į sutikimo, kaip teisinio pagrindo, svarbą visais pirmiau aprašytais atvejais ir į individualių teisių vaidmenį duomenų apsaugos teisinėje sistemoje, siekiant apsaugoti duomenų subjektų pagrindines teises ir laisves, EDAV ragina Europos Komisiją išsamiau įvertinti bendrosios teisės atšaukti sutikimą pagal Korėjos teisę nebuvimo poveikį ir pateikti papildomų garantijų, kad visada būtų garantuotas toks esminis duomenų apsaugos lygis, koks yra numatytas BDAR, taip pat, jei reikia, patikslinant teisės į duomenų tvarkymo sustabdymą vaidmenį šiomis konkrečiomis aplinkybėmis.

3.1.4. Tikslų apribojimo principas

68. BDAR darbiniame dokumente dėl referencinio tinkamumo, laikantis BDAR, numatyta, kad asmens duomenys turėtų būti tvarkomi konkrečiu tikslu ir vėliau naudojami tik tiek, kiek tai nėra nesuderinama su tvarkymo tikslu.

69. Pagal PIPA 3 straipsnio 1 ir 2 dalis asmens duomenų valdytojai nurodo ir paaiškina tvarkymo tikslus ir užtikrina, kad tvarkymas šiuos tikslus atitiktų. Nors šis principas yra patvirtintas kitose nuostatose (t. y.

[23] Nors duomenų subjektai tam tikromis aplinkybėmis gali atsisakyti duoti sutikimą, žr., pavyzdžiui, PIPA 18 straipsnio 3 dalies 5 punktą. Priešingai, teisė atšaukti sutikimą, atrodo, taikoma tik konkrečiais atvejais; pagal PIPA 27 straipsnio 1 dalį 2 punktą duomenų subjektai turi teisę atšaukti sutikimą, jei jie nenori, kad jų asmens duomenys būtų perduoti trečiajai šaliai dėl tam tikrų ar visų asmens duomenų, susijusių su valdytojo verslu, susijungimo ir pan. perdavimo; pagal PIPA 39 straipsnio 7 dalį naudotojai gali bet kada atšaukti informacijos ir ryšių paslaugų teikėjui duotą sutikimą dėl asmens duomenų rinkimo, naudojimo ir teikimo, ir pan.; ir pagal CIA 37 straipsnį individualus kredito informacijos subjektas gali atšaukti sutikimą, duotą kredito informacijos teikėjui ir (arba) naudotojui.

PIPA 15 straipsnio 1 dalyje, 18 straipsnio 1 dalyje ir 19 straipsnio 1 dalyje), tam tikromis aplinkybėmis leidžiama tvarkyti duomenis pagrįstai susijusiais tikslais (žr. PIPA 17 straipsnio 4 dalį)[24], taip pat netiksliniu būdu naudoti ir teikti asmens duomenis (žr. PIPA 18 ir 19 straipsnius)[25].

70. EDAV supranta, kad perduodant asmens duomenis iš EEE į Korėjos Respubliką remiantis sprendimu dėl tinkamumo, EEE duomenų valdytojų duomenų rinkimo tikslas yra tas, kuriuo duomenys yra perduodami ir taikytinas tvarkymui, kurį atlieka duomenis gaunantis Korėjos asmens duomenų valdytojas. Korėjos duomenų valdytojas galėtų pakeisti tikslą tik taip, kaip numatyta PIPA 18 straipsnio 2 dalies 1–3 punktuose, „*nebent tikėtina, kad tai padarius bus nesąžiningai pažeisti duomenų subjekto ar trečiosios šalies interesai*“[26]. Atsižvelgdama į tai, EDAV pripažįsta sprendimo projekto 55 konstatuojamojoje dalyje pateiktą Europos Komisijos pareiškimą, kad tais atvejais, kai pagal įstatymus leidžiama keisti tikslą, pagal šiuos įstatymus turi būti gerbiama pagrindinė teisė į privatumą ir duomenų apsaugą. Tačiau EDAV pažymi, kad nebuvo pateikta jokios konkrečios informacijos šiam teiginiui pagrįsti, pavyzdžiui, nebuvo padaryta nuoroda į (Korėjos) Konstitucijos 37 straipsnį. Todėl EDAV ragina Europos Komisiją sprendimo projekte pateikti papildomus patikinimus ir garantijas, siekiant užtikrinti, kad pagal visus įstatymus, pagal kuriuos leidžiama keisti tvarkymo tikslą, būtų gerbiamos duomenų subjektų pagrindinės teisės ir laisvės į privatumą ir duomenų apsaugą.

3.1.5. Duomenų kokybės ir proporcingumo principas

71. BDAR darbiniame dokumente dėl referencinio tinkamumo teigiama, kad duomenys turėtų būti tikslūs ir, jei reikia, nuolat atnaujinami. Duomenys turėtų būti tinkami, aktualūs ir ne pernelyg išsamūs atsižvelgiant į tikslus, kuriais jie yra tvarkomi.

72. Pagal PIPA asmens duomenų valdytojai turi užtikrinti, kad asmens duomenys būtų tikslūs, išsamūs ir atnaujinti tiek, kiek būtina, atsižvelgiant į tikslus, kuriais asmens duomenys yra tvarkomi (PIPA 3 straipsnio 3 dalis). Asmens duomenų valdytojai privalo surinkti tik tiek asmens duomenų, kiek būtina tam tikram tikslui pasiekti. Šiuo atžvilgiu jiems tenka prievolė įrodyti (PIPA 16 straipsnio 1 dalis).

73. Atsižvelgdama į tai, EDAV pritaria Europos Komisijos vertinimui dėl esminio PIPA apsaugos lygio lygiavertiškumo, palyginti su BDAR.

3.1.6. Duomenų saugojimo principas

74. Remiantis BDAR darbiniu dokumentu dėl referencinio tinkamumo, paprastai duomenys turėtų būti saugomi ne ilgiau, nei būtina tiems tikslams, kuriais asmens duomenys yra tvarkomi. Pagal PIPA 21 straipsnio 1 dalį šis principas egzistuoja ir Korėjos teisėje. Pagal PIPA asmens duomenų valdytojai privalo nedelsdami sunaikinti asmens duomenis, kai asmens duomenys tampa nereikalingi pasibaigus saugojimo laikotarpiui arba pasiekus numatytą tvarkymo tikslą, nebent būtų taikomi įstatymu nustatyti saugojimo laikotarpiai.

75. Tačiau EDAV kelia susirūpinimą tai, kad PIPA 21 straipsnio 1 dalis netaikoma pseudoniminiams asmens duomenims. EDAV atkreipia dėmesį į tai, kad pagal Pranešimo Nr. 2021-1 4 skyriaus iii punktą, *kai asmens duomenų valdytojas tvarko pseudoniminę informaciją, kad galėtų rinkti statistiką, atlikti mokslinius tyrimus, išsaugoti viešuosius įrašus ir pan. ir jei pseudoniminė informacija turi būti sunaikinta, kai pagal Konstitucijos 37 straipsnį ir Įstatymo 3 straipsnį (asmens duomenų apsaugos principai) pasiekiamas konkretus tvarkymo tikslas, jis anonimizuoja informaciją, siekdamas užtikrinti, kad pagal ją atskirai arba kartu su kita informacija nebebūtų nustatomas konkretus asmuo, pagrįstai*

[24] Todėl tikslo suderinamumas turi būti iš anksto nustatytas remiantis PIPA vykdymo dekreto 14 straipsnio 2 dalyje nustatytais kriterijais.
[25] Taip pat žr. pirmiau pateiktą 66 punktą.
[26] PIPA 18 straipsnio 2 dalis.

atsižvelgiant į laiką, sąnaudas, technologijas ir pan., pagal PIPA 58 straipsnio 2 dalį. Šiuo atveju taip pat atsižvelgiant į Pranešimo Nr. 2021-1 svarbą ir siekiant teisinio tikrumo dėl Korėjos Respublikai pagal sprendimą dėl tinkamumo perduotų asmens duomenų apsaugos lygio lygiavertiškumo, EDAV pakartoja savo raginimą Europos Komisijai pateikti papildomos informacijos, konkrečiai apie tai, kaip Pranešimas Nr. 2021-1 tampa privalomu ir kaip užtikrinamas jo įgyvendinamumas ir galiojimas[27].

3.1.7. Duomenų saugumo ir konfidencialumo principas

76. Kaip nurodyta BDAR darbiniame dokumente dėl referencinio tinkamumo, pagal saugumo ir konfidencialumo principą reikalaujama, kad duomenų tvarkymo subjektai įsitikintų, jog asmens duomenys, naudojant tinkamas technines ar organizacines priemones, yra tvarkomi taip, kad būtų užtikrintas jų saugumas, įskaitant apsaugą nuo tvarkymo neturint leidimo ar nuo neteisėto tvarkymo, taip pat nuo atsitiktinio duomenų praradimo, sunaikinimo ar sugadinimo. Užtikrinant saugumo lygį, turėtų būti atsižvelgiama į naujausias technologijas ir susijusias sąnaudas.

77. Europos Komisija aptiko panašų duomenų saugumo principą PIPA 3 straipsnio 4 dalyje, kuris išsamiau patikslintas PIPA 29 straipsnyje. Be to, duomenų saugumo nuostatos taikomos tuomet, kai asmens duomenų valdytojas pasitelkia „užsakomąjį subjektą“. Duomenų tvarkymo saugumas turi būti užtikrintas taikant technines ir valdymo apsaugos priemones, kurios taip pat turi būti įtrauktos į privalomą duomenų tvarkymo susitarimą (PIPA 26 straipsnis ir PIPA vykdymo dekreto 28 straipsnis). Be to, pagal PIPA taikomi konkretūs įpareigojimai duomenų pažeidimo atveju, įskaitant įpareigojimą pranešti nukentėjusiems duomenų subjektams ir priežiūros institucijai, kai paveiktų duomenų subjektų skaičius viršija taikytiną ribą (PIPA 34 straipsnis kartu su PIPA Prezidento dekreto 39 straipsniu), išskyrus atvejus, kai susiję duomenys yra pseudoniminiai asmens duomenys, tvarkomi siekiant statistikos, mokslinių tyrimų ar archyvavimo tikslų dėl viešojo intereso (PIPA 28 straipsnio 7 dalis). Šiuo atveju[28] EDAV taip pat yra susirūpinusi dėl plataus masto išimčių pseudoniminei informacijai ir pakartoja savo raginimą Europos Komisijai išsamiau įvertinti šį aspektą, siekiant, kad pagal Korėjos teisę būtų iš esmės užtikrinamas lygiavertis apsaugos lygis[29].

78. Nepaisant to, apibendrinant, EDAV yra patenkinta Europos Komisijos vertinimu ir išvada dėl esminio Korėjos teisės lygiavertiškumo saugumo ir konfidencialumo principo atžvilgiu.

3.1.8. Skaidrumo principas

79. Pagal BDAR 5 straipsnio 1 dalies a punktą, pagrindinis ES duomenų apsaugos sistemos principas yra skaidrumas. BDAR 39 konstatuojamojoje dalyje nurodoma esminė šio principo funkcija, teigiant, kad *„[t]aikant skaidrumo principą, fiziniams asmenims turėtų būti aišku, kaip su jais susiję asmens duomenys yra renkami, naudojami, su jais susipažįstama arba jie yra kitaip tvarkomi, taip pat kokiu mastu tie asmens duomenys yra ar bus tvarkomi. <...> Fiziniai asmenys turėtų būti informuoti apie su asmens duomenų tvarkymu susijusius pavojus, taisykles, apsaugos priemones bei teises ir apie tai, kaip naudotis savo teisėmis tokio asmens duomenų tvarkymo srityje.“*

80. BDAR darbiniame dokumente dėl referencinio tinkamumo skaidrumas aiškiai nurodomas kaip vienas iš turinio principų, į kurį reikia atsižvelgti vertinant esminį trečiosios šalies suteikiamos apsaugos lygio lygiavertiškumą. Konkrečiau jame teigiama, kad *„kiekvienas asmuo turėtų būti aiškiai, lengvai prieinamai, glaustai, skaidriai ir suprantamai informuotas apie visus pagrindinius jo asmens duomenų tvarkymo elementus. Tokia informacija turėtų apimti tvarkymo tikslą, duomenų valdytojo tapatybę, jam suteiktas teises ir kitą informaciją, kiek tai būtina sąžiningumui užtikrinti. Esant tam tikroms sąlygoms, gali būti kai kurių šios teisės į informaciją išimčių, pavyzdžiui, siekiant užtikrinti nusikaltimų*

[27] Taip pat žr. šioje nuomonėje pirmiau pateiktą 3.1.1.1 skyriaus 51 punktą, taip pat 52 punktą dėl EDAV bendro susirūpinimo dėl pseudonimų suteikimo pagal Korėjos teisę poveikio.
[28] Kaip jau nurodyta pirmiau šios nuomonės 3.1.1.1 skyriaus 51–52 dalyse.
[29] Taip pat žr. šios nuomonės 3.1.6 ir 3.1.10 skyrius.

tyrimus, nacionalinį saugumą, teismų nepriklausomumą ir teisminį procesą ar kitus svarbius visuotinės svarbos tikslus, kaip tai daroma BDAR 23 straipsnyje.“

81. Panašiai kaip ir BDAR atveju, pagal PIPA taikomas bendras skaidrumo principas, pagal kurį reikalaujama, kad asmens duomenų valdytojai viešai skelbtų savo privatumo politiką ir kitus su asmens duomenų tvarkymu susijusius klausimus (PIPA 3 straipsnio 5 dalis). Konkretūs informavimo įpareigojimai taikomi tuomet, kai asmens duomenų valdytojai siekia gauti duomenų subjektų sutikimą rinkti ir tvarkyti asmens duomenis (PIPA 15 straipsnio 2 dalis), dalytis asmens duomenimis su trečiąja šalimi (PIPA 17 straipsnio 2 dalis)) ir asmens duomenis tvarkyti netiksliniu būdu (PIPA 18 straipsnio 3 dalis). Reikia pažymėti, kad šie informavimo įpareigojimai taip pat *mutatis mutandis* taikomi užsakomajam subjektui (PIPA 26 straipsnio 7 dalis).

82. EDPB pripažįsta ir palankiai vertina Pranešimo Nr. 2021-1[30] 3 skyriaus i ir ii punktuose nurodytas papildomas apsaugos priemones, susijusias su informacija, kuri turi būti pateikta duomenų subjektams, kai jų duomenis perduoda EEE subjektas, atsižvelgiant į tai, kad pagal PIPA 20 straipsnio 1 dalį, kai duomenys nebuvo gauti iš duomenų subjekto, duomenų subjektai informuojami tik paprašius, o bendra teisė būti informuotam pripažįstama tik pagal PIPA 20 straipsnio 2 dalį, kai tam tikros tvarkymo operacijos viršija PIPA vykdymo dekrete nustatytas ribas (15 straipsnio 2 dalis).

83. Apskritai EDAV yra patenkinta, kad pagal Korėjos teisę skaidrumo principo atžvilgiu apsaugos lygis iš esmės yra lygiavertis pagal BDAR nustatytam apsaugos lygiui.

3.1.9. Specialios asmens duomenų kategorijos

84. Kad trečiosios šalies duomenų apsaugos sistema būtų pripažinta užtikrinanti asmens duomenų apsaugos lygį, iš esmės lygiavertį BDAR apsaugos lygiui, kai tvarkomi specialių kategorijų asmens duomenys, turėtų būti taikomos specialios apsaugos priemonės, kaip apibrėžta BDAR 9 ir 10 straipsniuose.

85. Pagal PIPA specialios nuostatos taikomos vadinamosios neskelbtinos informacijos, kuri apima asmens duomenis, atskleidžiančią ideologiją, įsitikinimus, priėmimą į profesinę sąjungą ar politinę partiją ar pasitraukimą iš jos, politines nuomones, sveikatą, lytinį gyvenimą ir kitus asmens duomenis, tvarkymui, kuris gali kelti didelę grėsmę bet kurio duomenų subjekto privatumui, taip pat, remiantis PIPA vykdymo dekretu, atliekant genetinius tyrimus gauta DNR informacija, duomenys apie teistumą, asmens duomenys, gauti specifinio techninio duomenų, susijusių su asmens fizinėmis, fiziologinėmis ar elgesio savybėmis, tvarkymo metu, siekiant unikaliai nustatyti to asmens tapatybę, ir asmens duomenys, atskleidžiantys rasinę ar etninę kilmę.

86. Kaip ir BDAR, Korėjos duomenų apsaugos įstatymais draudžiama tvarkyti neskelbtiną informaciją, nebent būtų taikomos specialios išimtys, kurias sudaro: 1) duomenų subjekto informavimas ir konkretaus sutikimo gavimas, ir 2) teisinės nuostatos, pagal kurias leidžiama tvarkyti duomenis (PIPA 23 straipsnio 2 dalis).

87. Šiuo pagrindu EDAV iš esmės sutinka su Europos Komisijos išvada dėl esminio Korėjos teisės lygiavertiškumo specialių kategorijų asmens duomenų tvarkymo atžvilgiu. Tačiau EDAV norėtų pažymėti, kad jai nebuvo pateiktas nei PIPA vadovas, nei PIPC patikslinimai dėl sąvokos „lytinis gyvenimas“, kuri aiškinama kaip apimanti ir asmens seksualinę orientaciją ar prioritetus ir kuri nebuvo įtraukta į Pranešimą Nr. 2021-1. Todėl EDAV ragina Europos Komisiją pateikti šią informaciją, kad ji galėtų nepriklausomai ją įvertinti. Be to, EDAV ragina Europos Komisiją konkrečiai nurodyti dokumentus, kuriuose galima rasti jos minimą informaciją šia tema.

[30] Sprendimo projekto I priedas.

3.1.10. Teisė susipažinti su duomenimis, juos ištaisyti, ištrinti ir pareikšti prieštaravimą

88. Korėjos teisinėje sistemoje duomenų subjekto teisės pripažįstamos PIPA 3 straipsnio 5 dalyje, pagal kurią asmens duomenų valdytojas garantuoja duomenų subjekto teises, išvardytas PIPA 4 straipsnyje ir išsamiau išdėstytas PIPA 35–37, 39 straipsniuose ir 39 straipsnio 2 dalyje, ir, dėl asmeninės kredito informacijos (t. y. informacijos, būtinos norint nustatyti finansinių ar komercinių sandorių šalių kreditingumą, žr. sprendimo projekto 3 konstatuojamąją dalį), – CIA 37 ir 38 straipsniuose ir 38 straipsnio 3 dalyje.

89. EDAV pažymi, kad teisė susipažinti su duomenimis (ir juos pataisyti bei ištrinti, kuria gali pasinaudoti „*duomenų subjektas, gavęs prieigą prie savo asmens duomenų pagal PIPA 35 straipsnį*“) gali būti apribota arba atimta, „*kai prieiga yra uždrausta arba apribota įstatymais*“, „*kai prieiga gali pakenkti trečiosios šalies gyvybei ar kūnui arba nepagrįstai pažeisti bet kurio kito asmens nuosavybę ir kitus interesus*“, ir be to, kalbant apie viešąsias institucijas, kai leidus susipažinti su duomenimis „*kiltų didelių sunkumų*“ vykdant tam tikras funkcijas, išsamiau nurodytas PIPA 35 straipsnio 4 dalyje[31]. Panašios nuostatos taip pat išdėstytos PIPA 37 straipsnyje, susijusiame su teise sustabdyti asmens duomenų tvarkymą.

90. Pagal BDAR 23 straipsnį Sąjungos ar valstybių narių teisėje leidžiama apriboti asmens teises, kai tokiu apribojimu gerbiama pagrindinių teisių ir laisvių esmė ir jis demokratinėje visuomenėje yra būtina ir proporcinga priemonė ir tokie apribojimai numatomi, be kita ko, siekiant apsaugoti duomenų subjektą arba kitų asmenų teises ir laisves ir užtikrinti „*stebėsenos, tikrinimo ar reguliavimo funkciją, kuri (net jeigu tik kartais) yra susijusi su viešosios valdžios funkcijų vykdymu a – e ir g punktuose nurodytais atvejais*“.

91. Atsižvelgiant į tai, EDAV palankiai vertintų, jei sprendimo projekte būtų bendrai patikinama, jog reikia, kad bet koks įstatymas ar statutas, ribojantis duomenų subjektų teises, atitiktų Korėjos konstitucijos reikalavimus, kad pagrindinė teisė gali būti apribota tik tada, kai tai būtina nacionaliniam saugumui užtikrinti arba viešajai tvarkai palaikyti visuomenės labui, ir kad šis apribojimas negali turėti įtakos atitinkamos laisvės ar teisės esmei (Korėjos Konstitucijos 37 straipsnio 2 dalis).

92. Be to, kalbant apie išimtį, kai prieiga prie duomenų gali „*nepagrįstai pažeisti bet kurio kito asmens nuosavybę ir kitus interesus*“, EDAV pripažįsta, kad tai „*reiškia, kad turėtų būti nustatyta pusiausvyra, viena vertus, tarp konstituciškai ginamų asmens teisių ir laisvių ir, kita vertus, kitų asmenų*[32]“, tačiau ji paragintų Europos Komisiją visapusiškai stebėti šios išimties taikymą ir atitinkamą teismų praktiką, siekiant užtikrinti, kad Korėjos teisinėje sistemoje taip pat praktiškai būtų užtikrintas lygiavertis duomenų subjektų teisių apsaugos lygis.

93. Taip pat EDAV palankiai vertintų, jei būtų atidžiai stebima, kaip viešosios įstaigos taiko šią išimtį, ypač tais atvejais, kai prieigos suteikimas būtų laikomas sukeliančiu „*didelius sunkumus*“ vykdant savo pareigas, atsižvelgiant į tai, kad ši sąvoka atrodo platesnė nei ta, kuri vartojama kitose PIPA nuostatose, pvz., 18 straipsnio 2 dalies 5 punkte[33], ir ji turėtų būti aiškinama siaurai, kad būtų išvengta nepagrįsto duomenų subjekto teisių apribojimo.

94. Be to, EDAV yra susirūpinusi dėl to, ar išimtys, pagal kurias nuostatos dėl skaidrumo gavus prašymą (PIPA 20 straipsnis) ir asmens teisių (PIPA 35–37 straipsniai) – taip pat panašios išimtys, susijusios su reikalavimais informacijos ir ryšių paslaugų teikėjams (PIPA 39 straipsnio 2 dalis ir 39 straipsnio 6–8

[31] Tos pačios PIPA numatytos teisės susipažinti su duomenimis ir juos ištaisyti sąlygos ir išimtys taip pat taikomos ir CIA numatytai teisei susipažinti su duomenimis ir juos ištaisyti, susijusiai su asmenine kredito informacija (sprendimo projekto 135 išnaša).

[32] Sprendimo projekto 76 konstatuojamoji dalis.

[33] Kalbant apie išimtis, taikomas asmens duomenų netikslinio naudojimo ir teikimo apribojimams, PIPA 18 straipsnio 2 dalies 5 punkte daroma nuoroda į situacijas, kai viešosioms institucijoms „*neįmanoma*“ vykdyti savo pareigų.

dalys) ir CIA (žr. 40 straipsnio 3 dalyje numatytas išimtis) – netaikomos pseudoniminei informacijai, kai ji yra tvarkoma statistikos, mokslinių tyrimų ar archyvavimo tikslais dėl viešojo intereso(PIPA 28 straipsnio 7 dalis), atitinka Europos teisinėje sistemoje numatytas apsaugos priemones.

95. Panašu, kad šiose nuostatose nustatoma bendra nukrypti leidžianti nuostata tokio tipo tvarkymui, o BDAR numatoma, kad tais atvejais, kai asmens duomenys (įskaitant pseudoniminius asmens duomenis) yra tvarkomi mokslo ar istorijos tyrimų ar statistikos tikslais, Sąjungos ar valstybių narių teisėje gali būti numatytos nukrypti nuo duomenų subjekto teisių leidžiančios nuostatos, tačiau tik „*tokiu mastu, kokiu dėl tokių teisių gali tapti neįmanoma pasiekti konkrečių tikslų arba jos gali tapti rimta kliūtimi jiems pasiekti, ir norint pasiekti tuos tikslus yra būtinos tokios nukrypti leidžiančios nuostatos*“, kai pseudonimų suteikimas yra tik viena iš techninių ir organizacinių priemonių, kurių reikia imtis siekiant užtikrinti, kad būtų laikomasi duomenų kiekio mažinimo principo (BDAR 89 straipsnio 1 dalis).

96. Europos Komisija mano, kad PIPA 28 straipsnio 7 dalyje numatyta nukrypti leidžianti nuostata yra taip pat pagrįsta atsižvelgiant į PIPA 28 straipsnio 5 dalį, pagal kurią asmens duomenų valdytojui aiškiai draudžiama tvarkyti pseudoniminę informaciją tam tikro asmens tapatybei nustatyti ir nurodomas BDAR 11 straipsnio 2 dalyje (kartu su BDAR 57 konstatuojamąja dalimi) išdėstytas požiūris į duomenų tvarkymą, kurio metu nereikia nustatyti tapatybės[34].

97. Iš tiesų, pagal BDAR 11 straipsnį duomenų valdytojas neprivalo „*laikyti, gauti ar tvarkyti papildomą informaciją duomenų subjekto tapatybei nustatyti*“ vien tam, kam būtų laikomasi BDAR, jei numatytais tikslais jis gali tvarkyti asmens duomenis, kuriems nereikia arba nebereikia nustatyti duomenų subjekto tapatybės; tokiais atvejais, kai duomenų valdytojas gali įrodyti, kad jis negali nustatyti duomenų subjekto tapatybės, duomenų subjekto teisės netaikomos. Kaip pripažino Europos Komisija[35], pagal BDAR tokiais atvejais reikalaujama, kad duomenų valdytojas „praktiškai“ negalėtų tvarkyti papildomos informacijos ir, laikantis duomenų kiekio mažinimo principo, pripažįstama, kad „dėl“ BDAR nereikia tvarkyti jokių papildomų duomenų.

98. Tačiau EDAV mano, kad ši situacija skiriasi nuo tos, kurioje duomenų valdytojas praktiškai gali nustatyti duomenų subjekto tapatybę, tačiau to daryti neleidžiama pagal teisės aktų, pavyzdžiui, PIPA 28 straipsnio 5 dalies, nuostatas. Šiuo atveju EDAV palankiai vertina Pranešime Nr. 2021-1 PIPC pateiktus paaiškinimus[36], patvirtinančius, kad PIPA 3 skyrius (įskaitant 28 straipsnio 7 dalį) ir 40 straipsnio 3 dalies išimtis taikomi tik tada, kai pseudoniminė informacija tvarkoma mokslinių tyrimų, statistikos ir archyvavimo tikslais dėl viešojo intereso. Tačiau be jau minėtų susirūpinimą keliančių klausimų dėl Pranešimo Nr. 2021-1 veiksmingo privalomojo pobūdžio[37], EDAV tebekyla klausimas, ar PIPA 28 straipsnio 7 dalyje ir CIA 40 straipsnio 3 dalyje numatytos nukrypti leidžiančios nuostatos galėtų būti laikomos būtinomis ir proporcingomis demokratinėje visuomenėje, jei jos riboja duomenų subjekto teises visais atvejais, kai tokiais tikslais tvarkoma pseudoniminė informacija, t. y., net tada, kai asmens duomenų valdytojas praktiškai gali nustatyti duomenų subjekto tapatybę ir, tikėtina, kad dėl teisių nebus neįmanoma pasiekti konkrečių tikslų arba nebus labai trukdoma tų tikslų siekti.

99. Visų pirma, EDAV yra susirūpinusi dėl to, kad šios nukrypti leidžiančios nuostatos nebūtų nepagrįstos ir kad jų nereikėtų toliau tikrinti, ypač jei jas taiko asmens duomenų valdytojas, kuris suteikia

[34] Reikia pažymėti, kad tie patys argumentai negalėtų būti taikomi CIA 40 straipsnio 3 dalyje numatytai išimčiai dėl pseudoniminės kredito informacijos tvarkymo, nes 40 straipsnio 2 dalies 6 punkte numatyta, kad: „*Kredito informacijos bendrovė ir kt. netvarko pseudoniminės informacijos taip, kad būtų galima nustatyti konkretaus asmens tapatybę, siekiant kokio nors pelno ar nesąžiningo tikslo*“, todėl galėtų būti leidžiama iš naujo nustatyti tapatybę sąžiningu tikslu, pvz. tenkinant duomenų subjekto prašymą.

[35] Žr. sprendimo projekto 82 konstatuojamąją dalį.

[36] Sprendimo projekto I priedo 4 skyrius.

[37] Žr. pirmiau 3.1.1.1 skyrių.

duomenims pseudonimus „*statistikos, mokslinių tyrimų ir archyvavimo tikslais dėl viešojo intereso ir pan.*“ pagal PIPA 28 straipsnio 2 dalį „*be duomenų subjektų sutikimo*“ (ir nepateikdamas PIPA 20 straipsnyje numatytos informacijos)[38], jei šis duomenų valdytojas saugo informaciją, leidžiančią iš naujo nustatyti tapatybę. Pagal BDAR asmenys turėtų turėti galimybę naudotis savo teisėmis dėl bet kokios informacijos, pagal kurią galima nustatyti jų tapatybę ar juos išskirti, net jei informacija laikoma pseudonimine, nebent taikomas jau minėtas BDAR 11 straipsnis. Šiuo atžvilgiu EDAV pažymi, kad tik tada, kai šie duomenys pateikiami trečiajai šaliai tais pačiais statistiniais, mokslinių tyrimų ir archyvavimo tikslais, informacija, kuri gali būti naudojama tam tikro asmens tapatybei nustatyti, neturėtų būti įtraukta ir todėl vien tik asmens duomenų valdytojas, kuriam pagal PIPA 28-2 straipsnio 2 dalį suteikiami pseudoniminiai duomenys, greičiausiai „praktiškai“ negalėtų be papildomos informacijos nustatyti duomenų subjekto tapatybės.

100. Trumpai tariant, atsižvelgiant į tai, kad, kaip pripažino Europos Komisija, „*užuot pseudonimų suteikimu pasikliovus kaip galima apsaugos priemone, pagal PIPA jis nustatomas kaip išankstinė sąlyga, kad būtų galima vykdyti tam tikrą duomenų tvarkymo veiklą statistikos, mokslinių tyrimų ir archyvavimo tikslais dėl viešojo intereso (pvz., kad būtų galima tvarkyti duomenis be sutikimo arba sujungti skirtingus duomenų rinkinius)*“[39], tačiau tokiais atvejais numatomi svarbūs duomenų subjektų teisių apribojimai, EDAV ragina Europos Komisiją išsamiau įvertinti nukrypti leidžiančias nuostatas, numatytas PIPA 28 straipsnio 7 dalyje ir CIA 40 straipsnio 3 dalyje, ir atidžiai stebėti jų taikymą bei atitinkamą teismų praktiką[40], siekiant užtikrinti, kad duomenų subjekto teisės nebūtų nepagrįstai apribotos, kai pagal sprendimą dėl tinkamumo perduoti asmens duomenys yra tvarkomi šiais tikslais, atsižvelgiant į tai, kad daugeliu atvejų šios teisės taip pat padeda duomenų valdytojui užtikrinti tvarkomų duomenų kokybę.

3.1.11. Tolesnio duomenų perdavimo apribojimai

101. BDAR darbiniame dokumente dėl referencinio tinkamumo paaiškinta, kad tolesnis duomenų perdavimas neturi sumažinti fizinių asmenų, kurių asmens duomenys perduodami pagal sprendimą dėl tinkamumo, apsaugos lygio ir todėl bet koks tolesnis perdavimas „*turėtų būti leidžiamas tik tada, kai tolesniam gavėjui (t. y. tolesnio duomenų perdavimo gavėjui) taip pat taikomos taisyklės (įskaitant sutarčių taisykles), užtikrinant tinkamą apsaugos lygį ir laikantis atitinkamų nurodymų, kai duomenys tvarkomi duomenų valdytojo vardu*“.

102. Kalbant apie tolesnį duomenų perdavimą užsakomiesiems subjektams (t. y „tvarkytojams“), įsisteigusiems kitose trečiosiose šalyse, EDAV atkreipia dėmesį į tai, kad Korėjos teisinėje sistemoje nėra specialių taisyklių, apimančių šiuos atvejus, ir kad, kaip mano Europos Komisija[41], Korėjos asmens duomenų valdytojas, naudodamasis teisiškai privaloma priemone, turi užtikrinti, kad būtų laikomasi PIPA nuostatų dėl užsakomųjų paslaugų (PIPA 26 straipsnis), ir jis bus atsakingas už asmens duomenis, kurie buvo perduoti užsakomosioms paslaugoms suteikti (PIPA 26 straipsnis).

103. Kalbant apie tolesnį duomenų perdavimą trečiosioms šalims (t. y. kitiems asmens duomenų valdytojams), pagal PIPA 17 straipsnio 3 dalį Korėjos asmens duomenų valdytojas turi informuoti duomenų subjektus apie duomenų perdavimą į užsienį ir gauti jų sutikimą ir jis „*nesudaro sutarties dėl tarpvalstybinio asmens duomenų perdavimo pažeidžiant PIPA*“. EDAV pažymi, kad pastaroji nuostata,

---

[38] Žr. PIPA 28 straipsnio 7 dalį, kaip paaiškinta Pranešime Nr. 2021-1, pagal kurią tam tikros PIPA numatytos apsaugos priemonės, t. y. „*20, 21, 27 straipsniai, 34 straipsnio 1 dalis, 35–37 straipsniai, 39 straipsnio 3 ir 4 dalys ir 39 straipsnio 6 – 8 dalys*“ netaikomi pseudoniminei informacijai, tvarkomai siekiant surinkti statistiką, atlikti mokslinius tyrimus, išsaugoti viešuosius įrašus ir kt.

[39] Sprendimo projekto 42 konstatuojamoji dalis.

[40] Žr., pavyzdžiui, iniciatyvos „Open Net“ konstitucinius sunkumus (informacija svetainėje https://opennet.or.kr/19909 pateikiama tik korėjiečių kalba).

[41] Sprendimo projekto 87 konstatuojamoji dalis.

kaip mano Europos Komisija[42], užtikrins, kad jokioje sutartyje dėl tarpvalstybinio duomenų perdavimo negalėtų būti įpareigojimų, prieštaraujančių PIPA nustatytiems reikalavimams asmens duomenų valdytojui, ir todėl galėtų būti laikoma apsaugos priemone, tačiau pagal ją nenumatomas joks įpareigojimas nustatyti apsaugos priemones, siekiant užtikrinti, kad gavėjas užtikrintų tokį patį apsaugos lygį, kokį suteikia PIPA. Todėl EDAV pripažįsta, kad informacija grindžiamas duomenų subjekto sutikimas paprastai bus naudojamas kaip Korėjos asmens duomenų valdytojo duomenų perdavimo trečiosios šalies duomenų gavėjui pagrindas.

104. Šiuo atžvilgiu sveikintini papildomi Pranešime Nr. 2021-1 PIPC pateikti paaiškinimai dėl pareigos informuoti asmenis apie trečiąją šalį, kuriai bus pateikti jų duomenys[43], nes tai, kaip pabrėžė Europos Komisija[44], padėtų EEE duomenų subjektams priimti informacija grindžiamą sprendimą dėl to, ar sutikti su užsienio paslaugų teikimu.

105. Tačiau, kaip taip pat buvo svarstyta Nuomonėje 28/2018 dėl Europos Komisijos įgyvendinimo sprendimo projekto dėl tinkamos asmens duomenų apsaugos Japonijoje, reikia pabrėžti, kad pagal BDAR duomenų subjektai turi būti aiškiai informuoti apie galimą tokio duomenų perdavimo riziką, kylančią dėl to, kad trečiojoje šalyje nėra tinkamos apsaugos ir prieš duodant sutikimą nėra tinkamų apsaugos priemonių. Tokiame pranešime turėtų būti, pavyzdžiui, pateikta informacija, kad trečiojoje šalyje gali nebūti priežiūros institucijos ir (arba) joje nenustatyti duomenų tvarkymo principai ir (arba) nenumatytos duomenų subjekto teisės[45]. EDAV nuomone, labai svarbu suteikti šią informaciją, kad duomenų subjektas, gerai žinodamas šiuos konkrečius faktus apie duomenų perdavimą, galėtų duoti informacija grindžiamą sutikimą[46]. Todėl EDAV yra susirūpinusi dėl Europos Komisijos išvadų, pateiktų sprendimo dėl tinkamumo projekte, susijusių su šios rūšies duomenų perdavimu. Duomenų subjektai paprastai nežino apie duomenų apsaugos sistemą trečiosiose šalyse. Taigi negalima daryti išvados, kad duomenų subjektas galėtų įvertinti duomenų perdavimo riziką žinodamas tik konkrečią paskirties šalį. Prieš duomenų subjektui duodant sutikimą, veikiau turi būti pateikta aiški informacija apie konkrečią tokio asmens duomenų perdavimo į šalį, esančią už Korėjos Respublikos teritorijos, riziką.

106. Taigi EDAV prašo Europos Komisijos užtikrinti, kad duomenų subjektui teikiama informacija „*apie perdavimo aplinkybes*“ apimtų informaciją apie galimą perdavimo riziką, kylančią dėl to, kad trečiojoje šalyje nėra tinkamos apsaugos ir tinkamų apsaugos priemonių. Tai svarbu EDAV, siekiant įvertinti, ar sutikimo reikalavimai iš esmės yra lygiaverčiai BDAR pateiktiems reikalavimams.

107. Be to, turint galvoje tai, kad sutikimas turi būti laisvai duodamas, grindžiamas informacija, konkretus ir nedviprasmiškas, EDAV palankiai vertintų sprendime dėl tinkamumo pateiktus patikinimus, kad, susiklosčius bet kuriai situacijai, kai pagal BDAR negalėtų būti duotas galiojantis sutikimas, pvz., dėl galios disbalanso, Korėjos asmens duomenų valdytojai neperduos asmens duomenų trečiajai šaliai trečiojoje valstybėje.

108. Tais atvejais, kai asmens duomenų valdytojas gali pateikti asmens duomenis trečiajai šaliai užsienyje be duomenų subjekto sutikimo, t. y., 1) jei asmens duomenys pateikiami pagal taikymo sritį, pagrįstai susijusią su pradiniu duomenų rinkimo tikslu pagal PIPA 17 straipsnio 4 dalį; ir 2) jei asmens duomenys gali būti pateikta trečiajai šaliai išimtiniais atvejais, nurodytais PIPA 18 straipsnio 2 dalyje, EDAV atkreipia dėmesį į Pranešimo Nr. 2021-1 2 skyriuje PIPC pateiktus paaiškinimus (ir palankiai vertina numatytą pareigą, tenkančią Korėjos duomenų valdytojui ir gavėjui užsienyje, pasitelkus teisiškai

[42] Sprendimo projekto 88 konstatuojamoji dalis.
[43] Ten pat.
[44] Ten pat.
[45] 2018 m. gegužės 25 d. EDAV gairės 2/2018 dėl nukrypti leidžiančių nuostatų pagal Reglamento (EB) 2016/679 49 straipsnį, p. 8.
[46] 2018 m. gegužės 25 d. EDAV gairės 2/2018 dėl nukrypti leidžiančių nuostatų pagal Reglamento (EB) 2016/679 49 straipsnį, p. 7.

privalomą priemonę (pvz., sutartį) užtikrinti lygiavertį PIPA apsaugos lygį, įskaitant duomenų subjekto teisių atžvilgiu).

3.1.12. Tiesioginė rinkodara

109. Remiantis BDAR 21 straipsnio 2 ir 3 dalimis bei BDAR darbiniu dokumentu dėl referencinio tinkamumo, duomenų subjektas visada turi turėti galimybę be jokio mokesčio prieštarauti duomenų tvarkymui profiliavimo ir tiesioginės rinkodaros tikslais.

110. Kalbant apie PIPA 37 straipsnyje numatytą teisę sustabdyti duomenų tvarkymą, EDAV pripažįsta, kad Europos Komisija mano, jog ši teisė taip pat taikoma tais atvejais, kai duomenys naudojami tiesioginės rinkodaros tikslais[47] Tačiau EDAV palankiai vertintų, jei sprendimo projekte būtų pateikta su šiuo vertinimu susijusi papildoma informacija ir patikslinimai (pvz., nuorodos į atitinkamą teismų praktiką ir pan.), ypač dėl praktinio teisės sustabdyti duomenų tvarkymą taikymo tiesioginės rinkodaros atveju. Šiuo atžvilgiu EDAV taip pat pabrėžtų, kad teisė prašyti kredito informacijos teikėjo ir (arba) naudotojo nebesusisiekti su klientu tam, kad jis būtų supažindinamas su produktais ar paslaugomis arba raginamas juos pirkti, yra aiškiai nustatyta CIA (37 straipsnio 2 dalyje).

111. Be to, kaip pripažino Europos Komisija[48], Korėjos teisinėje sistemoje tokiam tvarkymui paprastai reikalingas konkretus (papildomas) duomenų subjekto sutikimas (žr. PIPA 15 straipsnio 1 dalies 1 punktą ir 17 straipsnio 2 dalies 1 punktą).

112. Kadangi negalima atmesti galimybės, kad iš EEE perduoti asmens duomenys Korėjoje gali būti tvarkomi tokiais tikslais, EDAV taip pat palankiai vertintų sprendime dėl tinkamumo pateiktus patikslinimus dėl esamos duomenų subjekto teisės atšaukti sutikimą[49] ir dėl teisės reikalauti, kad asmens duomenys būtų ištrinti ir nebetvarkomi, kai tvarkymas yra grindžiamas sutikimu (pvz., jei tvarkoma rinkodaros tikslais) ir duomenų subjektas jį atsiėmė.

3.1.13. Automatizuotas sprendimų priėmimas ir profiliavimas

113. Kaip savo sprendimo projekte pripažino Europos Komisija[50], PIPA ir jo vykdymo dekrete nėra bendrųjų nuostatų, kuriomis sprendžiamas duomenų subjektui įtakos turinčių sprendimų klausimas ir kurios pagrįstos tik automatizuotu asmens duomenų tvarkymu. Vis dėlto Korėjos teisinėje sistemoje tokia teisė numatyta CIA, kuriame nustatytos automatizuotų sprendimų taisyklės (36 straipsnio 2 dalis), net jei atrodo, kad jų taikymas nepatenka į PIPC priežiūros sritį (ir, kaip tokios, nepatenka į šio sprendimo projekto taikymo sritį – žr. pirmiau 2.3.2 skyrių dėl sprendimo projekto taikymo srities).

114. Kaip jau svarstė 29 straipsnio darbo grupė[51] savo nuomonėje 1/2016 dėl privatumo skydo ir EDAV savo ankstesnėje nuomonėje dėl sprendimo dėl tinkamumo, susijusio su Japonija[52], didėjanti automatizuotų sprendimų priėmimo, profiliavimo ir dirbtinio intelekto svarba reikštų, kad šiuo atžvilgiu reikėtų laikytis didesnės apsaugos požiūrio. Priešingai Europos Komisijos argumentams[53], pagal kuriuos konkrečių automatizuotų sprendimų priėmimo taisyklių nebuvimas PIPA greičiausiai

[47] Sprendimo projekto 79 konstatuojamoji dalis.
[48] Ten pat.
[49] Taip pat žr. pirmiau pateiktą 67 dalį. Nors galimybė atšaukti sutikimą yra aiškiai numatyta CIA 37 straipsnio 1 dalyje, ši teisė konkrečioms aplinkybėms PIPA paminėta tik du kartus 27 straipsnio 1 dalies 2 punkte ir 39 straipsnio 7 dalyje.
[50] Žr. sprendimo projekto 81 konstatuojamąją dalį.
[51] Ši darbo grupė buvo įkurta pagal Direktyvos 95/46/EB 29 straipsnį. Tai buvo nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais. Grupės užduotys apibrėžtos Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje. Dabar 29 straipsnio darbo grupė tapo EDAV.
[52] Nuomonė 28/2018 dėl Europos Komisijos įgyvendinimo sprendimo dėl tinkamos asmens duomenų apsaugos Japonijoje projekto priimta 2018 m. gruodžio 5 d.
[53] Sprendimo projekto 81 konstatuojamoji dalis.

neturės įtakos Sąjungoje surinktų asmens duomenų apsaugos lygiui (kadangi bet kurį automatizuotu tvarkymu pagrįstą sprendimą paprastai priimtų duomenų valdytojas Sąjungoje, kuris palaiko tiesioginį ryšį su atitinkamu duomenų subjektu), EDAV mano, kad negalima atmesti galimybės, jog Korėjos asmens duomenų valdytojas galėtų naudotis automatizuotu sprendimų priėmimu tuo atveju, kai duomenys perduodami pagal sprendimą dėl tinkamumo (pavyzdžiui, užimtumo srityje, siekiant įvertinti darbo rezultatus, patikimumą, elgesį ir pan.).

115. Kuriamos naujos technologijos sudaro sąlygas įmonėms lengviau įdiegti arba apsvarstyti galimybę įdiegti automatizuotas sprendimų priėmimo sistemas, o tai gali susilpninti asmenų padėtį. Kai sprendimai, kuriuos priima tik šios automatizuotos sistemos, turi įtakos asmenų teisinei padėčiai arba daro jiems didelį poveikį (pavyzdžiui, įtraukiant juos į juodąjį sąrašą ir taip panaikinant jų teises), labai svarbu nustatyti pakankamas apsaugos priemones, įskaitant teisę būti informuotam apie konkrečias sprendimo priežastis ir susijusią logiką, ištaisyti netikslią ar neišsamią informaciją ir užginčyti sprendimą, jei jis buvo priimtas remiantis neteisingais faktais[54].

116. Šiomis aplinkybėmis EDAV reiškia susirūpinimą dėl to, kad PIPA nėra teisinių nuostatų dėl automatizuoto sprendimų priėmimo ir todėl ragina Europos Komisiją spręsti šį susirūpinimą keliantį klausimą ir šiuo požiūriu toliau stebėti Korėjos teisės aktų sistemos raidą.

3.1.14. Atskaitomybė

117. Korėjos teisinėje sistemoje yra kelios taisyklės, kuriomis siekiama užtikrinti, kad asmens duomenų valdytojai parengtų tinkamas technines ir organizacines priemones, reikalingas veiksmingam savo įsipareigojimų dėl duomenų apsaugos vykdymui, ir galėtų įrodyti šį reikalavimų laikymąsi, be kita ko, kompetentingai priežiūros institucijai. Visų pirma EDAV palankiai vertina tai, kad yra parengtos taisyklės, pagal kurias numatoma priimti vidinį valdymo planą (PIPA 29 straipsnis), įpareigojimas atlikti vadinamąjį poveikio privatumui vertinimą (toliau – **PIA**) tais atvejais, kai duomenų tvarkymas kelia didesnę galimų privatumo pažeidimų riziką (PIPA 33 straipsnio 1 dalis ir PIPA vykdymo dekreto 35 straipsnis), darbuotojų mokymo ir priežiūros taisyklės (PIPA 28 straipsnis), taip pat įpareigojimas paskirti privatumo pareigūną (PIPA 31 straipsnis kartu su PIPA vykdymo dekreto 32 straipsniu).

118. EDAV pritaria Europos Komisijos nuomonei, susijusiai su iš esmės lygiaverte apsauga, kurią jie užtikrina – net ir tais atvejais, kai atrodo, kad taisyklės santykinai skiriasi nuo tų, kurios nustatytos BDAR, pvz., nėra nuostatos, kurioje būtų nurodyta, kad privatumo apsaugos pareigūnas turi būti nepriklausomas, tačiau aiškiai nustatyta, kad jis turi teikti ataskaitas asmens duomenų valdytojo vadovybei (PIPA 31 straipsnio 4 dalis) ir kad jis, vykdydamas šias funkcijas, neturėtų patirti nepagrįstų nepatogumų (PIPA 31 straipsnio 5 dalis), – ir siūlytų, kad Europos Komisija, peržiūrėdama sprendimą dėl tinkamumo, stebėtų faktinį šių nuostatų taikymą, kad būtų galima įvertinti jų įgyvendinimo veiksmingumą.

3.2. Procedūriniai ir vykdymo užtikrinimo mechanizmai

119. EDAV pagal BDAR darbiniame dokumente dėl referencinio tinkamumo nustatytus kriterijus išanalizavo šiuos Korėjos duomenų apsaugos sistemos aspektus, kuriuos apima sprendimo projektas: ar egzistuoja ir efektyviai veikia nepriklausoma priežiūros institucija, ar yra sistema, užtikrinanti tinkamą atitikties lygį, ir sistema, suteikianti galimybę pasinaudoti tinkamais teisių gynimo mechanizmais bei EEE asmenis aprūpinanti priemonėmis, kad jie galėtų naudotis savo teisėmis ir siekti teisių gynimo nesusidurdami su sudėtingomis kliūtimis ginant teises administracine tvarka ir sprendimus apskundžiant teismine tvarka.

120. Remiantis BDAR VI skyriumi ir BDAR darbinio dokumento dėl referencinio tinkamumo 3 skyriumi, turi būti viena ar daugiau nepriklausomų priežiūros institucijų, kurioms pavesta stebėti ir užtikrinti

[54] WP 254, p. 7.

duomenų apsaugos ir privatumo nuostatų laikymąsi bei jų vykdymą trečiojoje šalyje, kad būtų pasiektas lygiavertis EEE apsaugos lygis.

121. Šiomis aplinkybėmis trečiosios šalies priežiūros institucija, vykdydama savo pareigas ir naudodamasi savo įgaliojimais, privalo veikti visiškai nepriklausomai ir nešališkai, ir tai darydama neturi prašyti ar priimti nurodymų. Be to, priežiūros institucija turėtų naudotis visais būtinais ir prieinamais įgaliojimais bei misijomis, kad galėtų užtikrinti duomenų apsaugos teisių laikymąsi ir skatintų informuotumą. Taip pat reikėtų apsvarstyti priežiūros institucijos personalo ir biudžeto klausimus. Priežiūros institucija taip pat gali pradėti procedūrą savo iniciatyva.

3.2.1. Kompetentinga nepriklausoma priežiūros institucija

122. Korėjos Respublikoje nepriklausoma institucija, atsakinga už PIPA stebėseną ir vykdymą, yra PIPC. PIPC sudaro vienas pirmininkas, pirmininko pavaduotojas ir septyni komisijos nariai. Pirmininką ir pirmininko pavaduotoją Ministro Pirmininko siūlymu skiria Prezidentas. Du iš Komisijos narių skiriami rekomendavus pirmininkui, du – rekomendavus politinės partijos, kuriai priklauso pirmininkas, atstovams ir trys kiti nariai – rekomendavus kitų politinių partijų atstovams (PIPA 7 straipsnio 2 dalies 2 punktas). PIPC padeda sekretoriatas (7 straipsnio 13 dalis) ir gali būti sudarytos pakomisės (sudarytos iš trijų Komisijos narių) smulkiems pažeidimams ir pasikartojantiems klausimams spręsti (PIPA 7 straipsnio 12 dalis).
123. Šia prasme EDAV pripažįsta, kad, nepaisant neseniai atlikto PIPC reorganizavimo, po kurio labai pasikeitė jos statusas ir įgaliojimai, PIPC dėjo daug pastangų kurdama reikiamą infrastruktūrą, kad būtų galima įgyvendinti PIPA ir jos naujausius pakeitimus. Tarp šių pastangų galima paminėti PIPC taisyklių nustatymą, gairių, skirtų PIPA aiškinimui, rengimą ir pagalbos linijos, skirtos konsultuoti verslo subjektus ir asmenis dėl duomenų apsaugos nuostatų, taip pat teikti tarpininkavimo paslaugas skundams nagrinėti, įsteigimą. PIPC užduotys visų pirma apima konsultavimą įstatymų ir reglamentų, susijusių su duomenų apsauga, klausimais, duomenų apsaugos politikos krypčių ir gairių kūrimą, asmenų teisių pažeidimų tyrimą, skundų nagrinėjimą ir tarpininkavimą ginčams, užtikrinimą, kad būtų laikomasi PIPA, švietimo ir propagavimo užtikrinimą duomenų apsaugos srityje ir keitimąsi informacija bei bendradarbiavimą su trečiųjų šalių duomenų apsaugos institucijomis[55].

124. Skyrimas į PIPC ir jo sudėtis yra reglamentuoti PIPA 7 straipsnio 2 dalyje. Nors PIPC priklauso Ministro Pirmininko jurisdikcijai (o pirmininką ir pirmininko pavaduotoją Ministro Pirmininko siūlymu skiria Prezidentas), teisinė sistema įpareigoja komisijos narius savo pareigas atlikti nepriklausomai, pagal įstatymus ir savo sąžinę. EDAV pripažįsta PIPA nustatytas institucines ir procedūrines apsaugos priemones, ypač 7 straipsnio 4–7 dalyse. Vis dėlto EDAV palankiai vertintų, jei Europos Komisija stebėtų bet kokius pokyčius, galinčius turėti įtakos Pietų Korėjos priežiūros institucijos narių nepriklausomumui.

125. Be to, sprendimo projekte dar nėra PIPC biudžeto analizės, įskaitant finansavimo šaltinius ir biudžeto skaidrumą. EDAV mano, kad į šį elementą, kuris yra paminėtas tiek BDAR 56 straipsnio 1 dalyje, tiek duomenų apsaugos procedūriniuose ir vykdymo užtikrinimo principuose bei mechanizmuose, kuriuos reikia apsvarstyti pagal BDAR darbinį dokumentą dėl referencinio tinkamumo kai vertinama šalies ar tarptautinės organizacijos sistema, privaloma nuodugniai atsižvelgti, nes tai yra ekonominių ir žmogiškųjų išteklių, kuriuos turi priežiūros institucija, kad galėtų nepriklausomai vykdyti savo įstatymu nustatytus duomenų apsaugos įsipareigojimus ir užduotis, rodiklis, todėl patartų Europos Komisijai išsamiau į tai atsižvelgti sprendimo projekte.

[55] PIPC užduotys ir įgaliojimai daugiausia nustatyti PIPA 7 straipsnio 8 ir 9 dalyse, taip pat 61–66 straipsniuose.

3.2.2. Duomenų apsaugos sistema, užtikrinanti gerą reikalavimų laikymąsi

126. Vykdymo srityje EDAV pripažįsta įvairius PIPC vykdymo įgaliojimus ir sankcijas, kaip numatyta PIPA ir CIA, ir atkreipia dėmesį į Pranešime Nr. 2021-1 pateiktus paaiškinimus, pagal kuriuos PIPA 64 straipsnio 1 dalyje ir CIA 45 straipsnio 4 dalyje[56] nurodytos sąlygos bus taikomos tuomet, kai pažeidžiamas bet kuris iš principų, teisių ir pareigų, įtrauktų į asmens duomenų apsaugos įstatymą. Tačiau ji rekomenduotų Europos Komisijai atidžiai stebėti, kaip praktiškai taikomi PIPC įgaliojimai įpareigoti pažeidėją imtis priemonių, kurios, jos manymu, yra tinkamos pagal CIA 64 straipsnio 1 dalyje arba 45 straipsnio 4 dalyje išvardytas priemones.

127. Be to, dėl taisomųjų veiksmų, numatytų PIPA 64 straipsnio 1 dalyje, nesilaikant taisomojo veiksmo, PIPC yra įgaliota skirti ne daugiau kaip 50 mln. Korėjos vonų (KRW) baudą (75 straipsnio 2 dalies 13 punktas). Ši suma atitinka 36 564 EUR. EDAV mano ir yra susirūpinusi, kad tokios ribotos piniginės sankcijos gali neturėti ypač stipraus atgrasančio poveikio pažeidėjams, kaip numatyta įstatyme, siekiant užtikrinti duomenų apsaugos taisyklių vykdymą, nes neatrodo, kad tai būtų tikrai pakankama atgrasymo priemonė, ypač didelių organizacijų ar įmonių, turinčių didelius finansinius išteklius, atveju.

128. Kalbant apie tai, kad PIPC gali pareikalauti, jog centrinės administracinės agentūros vadovas ištirtų asmens duomenų valdytojo veiklą arba kartu pradėtų tyrimą dėl PIPA pažeidimų ir netgi nustatytų taisomuosius veiksmus jų jurisdikcijai priklausančių asmens duomenų valdytojų atžvilgiu (PIPA 63 straipsnio 4 ir 5 dalys), EDAV pažymi, kad nors sprendimo projekto 122 konstatuojamojoje dalyje buvo pateikta tam tikra informacija, apskritai šių kitų agentūrų pobūdis ir jų teisiniai santykiai su PIPC tebėra gana neaiškūs. Be to, PIPA 68 straipsnio 1 dalyje kalbama apie daug subjektų, kuriems būtų galima perduoti PIPC įgaliojimus. Net jei atrodo, kad ši nuostata buvo taikoma tik Korėjos interneto ir saugumo agentūrai[57], EDAV palankiai vertintų paaiškinimus dėl galimos šių subjektų sąveikos pobūdžio ir atidžią šios nuostatos taikymo ateityje stebėseną, siekiant užtikrinti subjektų, kuriems pavesta taikyti duomenų apsaugos taisykles, nepriklausomumą.

129. Kalbant apie sankcijas, panašu, kad Korėjos sistemoje derinamos skirtingų rūšių sankcijos, pradedant taisomaisiais veiksmais ir administracinėmis baudomis, baigiant baudžiamosiomis sankcijomis, kurios gali turėti stiprų atgrasomąjį poveikį, ir Korėjos valdžios institucijos pateikė kelis neseniai PIPC paskirtų baudų pavyzdžius, *inter alia*, 2020 m. gruodžio mėn. 6,7 mlrd. KRW bauda buvo paskirta vienai bendrovei už skirtingų PIPA nuostatų pažeidimą, o 2021 m. balandžio 28 d. kita 103,3 mln. KRW bauda paskirta įmonei „AI Technology“ už duomenų tvarkymo teisėtumo taisyklių, visų pirma dėl sutikimo, pažeidimą ir pseudoniminės informacijos tvarkymą.

130. Nors pirmiau minėtos sumos gali turėti atgrasomąjį poveikį, EDAV norėtų gauti papildomos informacijos apie metodą, kurį PIPC taikė administracinių baudų dydžiui apskaičiuoti, pavyzdžiui, baudų, paskirtų už taisomųjų veiksmų, nustatytų pagal PIPA 64 straipsnio 1 dalį nesilaikymą (žr. 75 straipsnio 2 dalies 13 punktą). Tai ypač svarbu kalbant apie baudžiamąsias sankcijas ir (Korėjos) baudžiamojo įstatymo taikymą.

3.2.3. Duomenų apsaugos sistema turi teikti paramą ir padėti duomenų subjektams naudotis savo teisėmis ir tinkamais teisių gynimo mechanizmais

131. Kalbant apie teisių gynimą, atrodo, kad Korėjos sistemoje siūlomi įvairūs būdai tinkamai apsaugai užtikrinti ir, visų pirma, asmens teisėms įgyvendinti, ginant teises administracine tvarka ir sprendimus apskundžiant teismine tvarka, įskaitant patirtos žalos atlyginimą.

[56] Tai yra, *„teisės pažeidimas laikomas pažeidžiančiu asmenų teises ir laisves asmens duomenų atžvilgiu ir nesiėmus veiksmų gali būti padaryta žala, kurią sunku ištaisyti“.*

[57] Žr. sprendimo projekto 117 konstatuojamąją dalį ir vykdymo dekreto 62 straipsnį.

132. Korėjos sistemoje, be administracinių ir teisminių būdų, taip pat siūlomi alternatyvūs mechanizmai, kuriais asmenys gali naudotis, kad apgintų savo teises, kaip paaiškinta sprendimo projekto 132 ir 133 konstatuojamosiose dalyse, atitinkamai susijusiose su Privatumo skambučių centru ir Tarpininkavimo ginčuose komitetu. Kadangi tai yra papildomi teisių gynimo būdai, EDAV norėtų išsamesnių paaiškinimų dėl to, kaip jie papildo duomenų subjektų, kurių asmens duomenys perduodami Korėjai pagal sprendimą dėl tinkamumo, teisių gynimo galimybes PIPC ir teismuose.

4. PRIEIGA PRIE ASMENS DUOMENŲ, VIEŠŲJŲ INSTITUCIJŲ PERDUOTŲ IŠ EUROPOS SĄJUNGOS, IR JŲ NAUDOJIMAS PIETŲ KORĖJOJE

133. Kalbant apie duomenų apsaugos lygį teisėsaugos ir nacionalinio saugumo srityse, Europos Komisija savo sprendimo projekte ir prieinamuose prieduose pateikė išsamią informaciją. Todėl EDAV šioje nuomonėje susilaiko nuo daugumos faktinių išvadų ir vertinimų pakartojimo.

134. Europos Komisija daro išvadą, kad pirmiau minėtose srityse užtikrinamas duomenų apsaugos lygis atitinka ESTT praktikoje nustatytus reikalavimus, todėl gali būti laikomas iš esmės lygiaverčiu Europos Sąjungos duomenų apsaugos lygiui.

135. Kalbant bendrai, EDAV norėtų pabrėžti, kad net tais atvejais, kai atrodo ar kai Europos Komisija tvirtina, jog iš ES į Pietų Korėją perduotiems duomenims atitinkamas Korėjos įstatymas greičiausiai neturės įtakos, vis tiek reikia tokiais atvejais įvertinti Korėjos duomenų apsaugos lygio tinkamumą. Jų aktualumą rodo ir tai, kad pati Europos Komisija juos nagrinėjo sprendimo projekte.

4.1. Bendra duomenų apsaugos sistema, susijusi su vyriausybės prieiga

136. Kalbant apie valdžios institucijų prieigą prie asmens duomenų, reikia panagrinėti įvairius Korėjos įstatymus, kad būtų galima įvertinti teisės į privatumą ir duomenų apsaugos lygį. Visų pirma, EDAV pažymi, kad PIPA, kaip pagrindinis duomenų apsaugos įstatymas, turi būti taikomas plačiai. Tačiau, nors PIPA yra visapusiškai taikomas teisėsaugos srityje, jo taikymas duomenų tvarkymui nacionalinio saugumo tikslais yra ribotas. Pagal PIPA 58 straipsnio 1 dalies 2 punktą III–VII skyriai netaikomi asmens duomenų tvarkymui nacionalinio saugumo tikslais. Tačiau I, II, IX ir X skyriai yra taikomi nacionalinio saugumo srityje. Taigi nacionalinių saugumo institucijų prieigai prie asmens duomenų ir jų naudojimui yra taikomi esminiai PIPA principai ir pagrindinės duomenų subjekto teisių garantijos bei nuostatos dėl priežiūros, vykdymo ir taisomųjų veiksmų.

137. Pietų Korėjos konstitucija taip pat įtvirtina esminius duomenų apsaugos principus, būtent teisėtumo, būtinumo ir proporcingumo principus. Šie principai taip pat taikomi Pietų Korėjos valdžios institucijų prieigai prie asmens duomenų teisėsaugos ir nacionalinio saugumo srityse[58].

138. Teisėsaugos srityje policija, prokurorai, teismai ir kitos viešosios įstaigos gali rinkti asmens duomenis, remdamiesi konkrečiais teisės aktais, t. y. Baudžiamojo proceso įstatymu (toliau – **CPA**), Ryšių privatumo apsaugos įstatymu (toliau – **CPPA**), Telekomunikacijų verslo įstatymu (toliau – **TBA**) ir Įstatymu dėl ataskaitų teikimo ir nurodytos finansinių operacijų informacijos naudojimo (toliau – **ARUSFTI**), kurie taikomi baudžiamojo persekiojimo ir pinigų plovimo bei teroristų finansavimo prevencijos srityse. Šiais konkrečiais įstatymais nustatyti papildomi apribojimai, apsaugos priemonės ir išimtys.

[58] Žr. sprendimo projekto 145 konstatuojamąją dalį.

139. Nacionalinio saugumo srityje, remiantis Nacionalinės žvalgybos tarnybos įstatymu (toliau – **NISA**) ir kitais nacionalinio saugumo įstatymais[59], Nacionalinė žvalgybos tarnyba (toliau – **NIS**) gali rinkti asmens duomenis ir perimti ryšių duomenis. Vykdydama savo įgaliojimus EDAV supranta, kad NIS turi atitikti pirmiau minėtas teisines nuostatas, taip pat PIPA nuostatas.

140. EDAV prašo Komisijos patikslinti, ar Korėjoje, be NIS, yra ir kitų institucijų, atsakingų už nacionalinio saugumo sritį, nes, atrodo, kad I priedo 6 skyriuje Europos Komisija pateikia NIS kaip nacionalinių saugumo agentūrų pavyzdį.

4.2. Ryšio patvirtinimo duomenų apsauga ir apsaugos priemonės, susijusios su vyriausybės prieiga teisėsaugos tikslais

141. Teisėsaugos institucijos, remdamosi atitinkamu įstatymu, CPPA, gali imtis dviejų rūšių priemonių, skirtų prieigai prie ryšių informacijos. Pagal CPPA atskiriamos ryšį ribojančios priemonės, kurios apima tiek įprasto pašto turinio rinkimą, tiek tiesioginį telekomunikacijų turinio perėmimą[60], ir vadinamųjų ryšio patvirtinimo duomenų rinkimas. Pastarasis apima telekomunikacijų datą, jų pradžios ir pabaigos laiką, siunčiamų ir gaunamų skambučių skaičių, taip pat kitos šalies abonento numerį, naudojimo dažnumą, telekomunikacijų paslaugų naudojimo žurnalo failus ir vietos nustatymo informaciją.[61]

142. EDAV pažymi, kad, panašu, jog ryšio patvirtinimo duomenims netaikomos tos pačios apsaugos priemonės, kaip duomenims, surinktiems taikant ryšį ribojančias priemones, t. y. turinio duomenims. Iš tikrųjų EDAV pastebi, kad renkant turinį yra taikoma daugiau apsaugos priemonių nei renkant ryšio patvirtinimo duomenis teisėsaugos tikslais: Pirma, skirtingai nuo turinio duomenų rinkimo, ryšio patvirtinimo duomenų rinkimas neapsiriboja tik tam tikrų sunkių nusikaltimų tyrimu, bet gali būti atliekamas, kai manoma, kad tai būtina „bet kokiam tyrimui ar bausmei vykdyti“ (CPPA 13 straipsnio 1 dalis). Antra, ryšio patvirtinimo duomenų rinkimas iš esmės nėra struktūrizuojamas kaip kraštutinė priemonė ir naudojamas tik tada, kai sunku kitaip užkirsti kelią nusikaltimui, suimti nusikaltėlį ar surinkti įrodymus.[62] Ryšio patvirtinimo duomenys gali būti renkami, kai prokuroras ar teisminės policijos pareigūnas „mano, kad tai būtina“ tiriant nusikaltimą ar vykdant bausmę. Tačiau šiuo požiūriu yra išimtis, taikoma stebėjimo tikruoju laiku duomenims ir ryšio patvirtinimo duomenims, susijusiems su konkrečia bazine radijo ryšio stotimi pagal CPPA 13 straipsnio 2 dalį. Trečia, ryšių turinio duomenis renkančios teisėsaugos agentūros turi nedelsdamos nustoti tai daryti, kai laikoma, kad tolesnė prieiga nebėra būtina[63]. Kalbant apie ryšio patvirtinimo duomenis, tai bent jau nėra aiškiai nurodyta CPPA ar jo vykdymo dekrete.

143. EDAV atkreipia dėmesį, kad ryšio patvirtinimo duomenys gali būti renkami tik remiantis teismo išduotu orderiu. Be to, pagal CPPA reikalaujama, kad tiek paraiškoje dėl orderio, tiek pačiame orderyje būtų pateikta išsami informacija[64]. Toks išankstinis teisminis leidimas padeda apriboti teisėsaugos institucijų diskreciją taikant įstatymus ir patikrinti, ar kiekvienu atveju yra pakankamų priežasčių ryšio patvirtinimo duomenims rinkti. EDAV taip pat pripažįsta, kad Korėjos Respublikos įstatymai, atrodo, nenumato bendro ir besąlygiško ryšio patvirtinimo duomenų saugojimo. Taigi vyriausybės prieiga prie tokių duomenų visada yra susijusi su duomenimis, kurie vis dar saugomi atsiskaitymo ir pačių ryšių paslaugų teikimo tikslais.

---

[59] Tarp nacionalinio saugumo įstatymų yra, pavyzdžiui, Ryšių privatumo apsaugos įstatymas, Kovos su terorizmu piliečių apsaugai ir visuomenės saugumui įstatymas arba Telekomunikacijų verslo įstatymas.
[60] CPPA 3 straipsnio 2 dalis, 2 straipsnio 6 ir 7 dalys.
[61] CPPA 2 straipsnio 11 dalis.
[62] Tai taikoma turinio duomenims pagal CPPA 3 straipsnio 2 dalį ir 5 straipsnio 1 dalį.
[63] CPPA vykdymo dekreto 2 straipsnis.
[64] Žr. sprendimo projekto 156 konstatuojamąją dalį.

144. Tačiau EDAV pabrėžia, kad ESTT suabejojotuo, kad srauto duomenys yra mažiau neskelbtini nei kiti, ir ypač – nei turinio duomenys[65]. Atsižvelgdama į tai, kad ryšio patvirtinimo duomenims keliais atžvilgiais suteikiama mažesnio lygio apsauga nei turinio duomenims, EDAV ragina Europos Komisiją atidžiai stebėti, ar pagal Korėjos teisę nustatytos tokios kategorijos asmens duomenų apsaugos priemonės užtikrina iš esmės lygiavertį apsaugos lygį tam, kuris garantuojamas ES, visų pirma atsižvelgiant į teisės proporcingumą ir numatomumą.

4.3. Korėjos valdžios institucijų prieiga prie ryšių informacijos nacionalinio saugumo tikslais

145. Kalbant apie teisinę sistemą, pagal kurią nacionalinės saugumo institucijos gali naudotis iš EEE į Korėją perduodama ryšių informacija, EDAV nustatė du susirūpinimą keliančius klausimus, kurie abu yra susiję su prieigos prie ne Korėjos piliečių ryšių informacijos, kuriai taikomas konkretus naudojimo atvejų rinkinys, tvarka (žr. 29 dalį). Tokiais atvejais tiek ryšio patvirtinimo, tiek turinio duomenims netaikomos tam tikros kitiems atvejams nustatytos apsaugos priemonės. Kitaip tariant, šiais konkrečiais atvejais šiems duomenims netaikomos tos pačios apsaugos priemonės, kaip ryšių duomenims, kai ryšyje dalyvauja bent vienas Korėjos pilietis.

4.3.1. Neprivaloma pranešti asmenims apie vyriausybės prieigą prie užsienio piliečių ryšių informacijos

146. Pagal pirmiau aprašytą atvejį, t. y. kai nė viena ryšių šalis nėra Korėjos pilietis, nacionalinės saugumo institucijos neprivalo pranešti asmenims apie jų duomenų rinkimą ir tvarkymą. EDAV pripažįsta, kad šis klausimas turi įtakos tik tam tikrais atvejais. Pirma, kaip jau buvo nurodyta, kai bent vienas Korėjos pilietis dalyvauja ryšyje, pranešimo reikalavimai pagal CPPA taikomi visoms ryšio šalims, nepriklausomai nuo jų pilietybės[66]. Antra, renkant asmens duomenis, gaunamus iš ryšio tik tarp užsienio piliečių, taikomas konkretus naudojimo atvejų rinkinys. Visų pirma, teisė į prieigą prie duomenų tokiais atvejais taikoma a) Korėjos Respublikai priešiškų šalių, b) užsienio agentūrų, grupių ar piliečių, įtariamų antikorėjietiškos veiklos vykdymu[67] arba c) grupių, veikiančių Korėjos pusiasalyje, bet faktiškai nepriklausančių Korėjos Respublikos suverenitetui, nariai ir jų susivienijimo grupių, įsikūrusių užsienio šalyse, ryšiams. Taigi iš EEE į Korėją perduotą ES asmenų ryšių informaciją galima rinkti tik nacionalinio saugumo tikslais, jei ji patenka į vieną iš trijų pirmiau minėtų kategorijų[68]. EDAV iš papildomų Europos Komisijos paaiškinimų suprato dar vieną ribojantį veiksnį, t. y. kad taikytinoje teisinėje sistemoje nenumatomas už Korėjos ribų perduodamų duomenų perėmimas.

147. Taigi pranešimo reikalavimo nebuvimo svarba, atsižvelgiant į jo praktinį poveikį, gali būti laikoma ribota. Tačiau EDAV pabrėžia (vėlesnio) pranešimo apie vyriausybės prieigą svarbą, ypač užtikrinant veiksmingas teisių gynimo priemones. Remiantis ESTT, pranešimas yra būtinas, kad nukentėję „*asmenys galėtų pasinaudoti iš Chartijos 7 ir 8 straipsnių išplaukiančiomis teisėmis prašyti leisti*

---

[65] Žr. 2020 m. spalio 6 d. ESTT sprendimo *Privacy International*, C-623/17, ECLI:EU:C:2020:790, 71 punktą. *Chartijos 7 straipsnyje įtvirtintos teisės suvaržymas, kurį lemia srauto ir vietos nustatymo duomenų perdavimas saugumo ir žvalgybos tarnyboms, turi būti laikomas ypač dideliu, atsižvelgiant, be kita ko, į informacijos, kurią gali atskleisti šie duomenys, jautrumą ir, be kita ko, į galimybę remiantis šiais duomenimis nustatyti duomenų subjektų profilį, nes tokia informacija yra tokia pat jautri kaip ir pats pranešimų turinys. Be to, toks suvaržymas duomenų subjektams gali sudaryti įspūdį, kad jų privatus gyvenimas yra nuolat stebimas (pagal analogiją žr. 2014 m. balandžio 8 d. Sprendimo Digital Rights Ireland ir kt., C-293/12 ir C-594/12, EU:C:2014:238, 27 ir 37 punktus ir 2016 m. gruodžio 21 d. Sprendimo Tele2, C-203/15 ir C-698/15, EU:C:2016:970, 99 ir 100 punktus).*

[66] Žr. sprendimo projekto 192 konstatuojamąją dalį.

[67] Žr. II priedo 244 išnašą, pagal kurią antikorėjietiškos veiklos sąvoka reiškia veiklą, kuri kelia grėsmę tautos egzistavimui ir saugumui, demokratinei tvarkai arba žmonių išlikimui ir laisvei.

[68] Žr. sprendimo projekto 187 konstatuojamąją dalį.

susipažinti su savo asmens duomenimis, kuriems taikomos šios priemonės, ir prireikus juos ištaisyti ar pašalinti, taip pat pagal Chartijos 47 straipsnio pirmą pastraipą pasinaudoti veiksminga teisine gynyba teisme“[69]. Vyriausybės prieiga nacionalinio saugumo tikslais dažnai apima slaptas stebėjimo priemones, o tai reiškia, kad stebėjimo objektai, duomenų subjektai, nežino, kad yra tvarkomi jų duomenys. Taigi, „*iš esmės suinteresuotam asmeniui yra mažai galimybių kreiptis į teismą, nebent jis informuojamas apie priemones, kurių imtasi jam nežinant, ir taip jam sudaroma galimybė ginčyti jų teisėtumą atgaline data, arba bet kuris asmuo, įtariantis, kad jo komunikacija yra ar buvo perimta, gali kreiptis į teismą, ir todėl teismų jurisdikcija nepriklauso nuo perėmimo subjekto informavimo apie jo komunikacijos perėmimą*“[70]. Atsižvelgiant į tai ir laikantis nuoseklumo, EDAV daug kartų išreiškė susirūpinimą dėl veiksmingų taisomųjų veiksmų stebėjimo atvejais. EDAV pabrėžia, kad vyriausybės priemonių slaptumas neturi lemti to, kad tokios priemonės būtų faktiškai neginčijamos. Šiomis aplinkybėmis, neatsižvelgiant į tai, ar pranešimo reikalavimo, susijusio su užsienio piliečių ryšių informacija, nebuvimas turi įtakos sprendimo projekte įvertintam duomenų apsaugos lygiui, jis turi būti vertinamas kaip bendro vertinimo dalis, ypač atsižvelgiant į pagal Korėjos teisę nustatytus priežiūros ir teisių gynimo mechanizmus (žr. 4.7 ir 4.8 skyrius).

148. Be to, šiomis aplinkybėmis EDAV atkreipia dėmesį į tai, kad įstatyme nurodomos gana plačios sąvokos, pvz., antikorėjietiška ar antinacionalinė veikla[71], ir kad sunku numatyti, kaip šios sąvokos aiškinamos pagal Korėjos teisę. EDAV ragina Europos Komisiją stebėti, kaip šios sąvokos yra įtvirtintos Korėjos teisėje ir ar jų taikymas praktikoje atitinka ES teisės aktuose nustatytus proporcingumo reikalavimus.

4.3.2. Nėra išankstinio nepriklausomo leidimo rinkti užsienio piliečių ryšių informaciją

149. Tais atvejais, kai EEE asmens duomenys, gauti iš ne Korėjos piliečių ryšių (ir patenkantys į vieną iš pirmiau minėtų naudojimo atvejų), turi būti tvarkomi Korėjoje nacionalinio saugumo tikslais, renkant tokius duomenis nereikia nepriklausomo organo išankstinio patvirtinimo (kaip ir ryšių atveju, kai bent vienas iš susijusių asmenų yra Korėjos pilietis).[72]

150. Ypač atsižvelgiant į neseniai priimtus Europos žmogaus teisių teismo (**EŽTT**) sprendimus *Big Brother Watch ir kt. prieš UK* ir *Centrum för Rättvisa prieš Švediją*, EDAV mano, kad būtina ištirti, ar tai yra esminis Korėjos duomenų apsaugos sistemos trūkumas. Šiuo atžvilgiu EDAV primena, kad, kaip pabrėžta jos atnaujintose rekomendacijose dėl Europos pagrindinių garantijų taikant stebėjimo priemones[73], Europos Sąjungos sutarties 6 straipsnio 3 dalyje nustatyta, kad EŽTK įtvirtintos pagrindinės teisės yra bendrieji ES teisės principai, nors, kaip primena ESTT savo praktikoje, pastaroji, kol Europos Sąjunga prie jos neprisijungia, nėra oficialiai į ES teisę įtraukta teisinė priemonė[74]. Taigi pagrindinių teisių apsaugos lygis, kurio reikalaujama BDAR 45 straipsnyje, turi būti nustatytas remiantis šio reglamento nuostatomis, aiškinamomis atsižvelgiant į Chartijoje įtvirtintas pagrindines teises. Todėl pagal Chartijos 52 straipsnio 3 dalį, joje nurodytos teisės, kurios atitinka EŽTK garantuojamas teises, turi turėti tą pačią reikšmę ir taikymo sritį, kaip šioje Konvencijoje nustatytos

[69] 2020 m. spalio 6 d. ESTT sprendimas *La Quadrature du Net ir kiti* sujungtose bylose C-511/18, C-512/18 ir C-520/18, ECLI:EU:C:2020:791, 190 punktas.

[70] 2021 m. gegužės 25 d. EŽTT sprendimas *Big Brother Watch ir kiti prieš UK*, ECLI:CE:ECHR:2021:0525JUD005817013, 337 punktas ir 2015 m. gruodžio 4 d. EŽTT sprendimas *Case of Roman Zakharov prieš Russia*, ECLI:CE:ECHR:2015:1204JUD004714306, 234 punktas.

[71] Europos Komisija paaiškino, kad, remiantis Korėjos vyriausybės paaiškinimais, tai reiškia „veiklą, keliančią grėsmę šalies egzistavimui ir saugumui, demokratinei tvarkai arba žmonių išlikimui ir laisvei“, taip pat žr. sprendimo dėl tinkamumo projekto 319 išnašą.

[72] Žr. sprendimo projekto 190 konstatuojamąją dalį.

[73] EDAV rekomendacijos Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones, 10 ir 11 dalys.

[74] Žr. 2020 m. liepos 16 d. ESTT sprendimo *Data Protection Commissioner prieš Facebook Ireland Ltd. ir Maximilian Schrems*, C-311/18, ECLI:EU:C:2020:559 (toliau –“*Schrems II*”), 98 punktą.

teisės. Todėl į EŽTT praktiką, susijusią su teisėmis, kurios taip pat numatytos Chartijoje, reikia atsižvelgti kaip į minimalią apsaugos ribą aiškinant atitinkamas teises Chartijoje, t. y. tiek, kiek Chartija, kaip aiškino ESTT, nenumato aukštesnio apsaugos lygio[75].

151. EDAV pažymi, kad nors išankstinis (nepriklausomas) stebėjimo priemonių patvirtinimas laikomas svarbia apsaugos nuo savivalės priemone, toks patvirtinimas negali būti kildinamas iš ESTT praktikos kaip absoliutus stebėjimo priemonių proporcingumo reikalavimas. Tačiau dabar EŽTT aiškiai nustatė reikalavimą gauti *ex ante* nepriklausomą leidimą masiniam duomenų perėmimui[76]. Nors sprendimo projekte tai aiškiai nenurodyta, EDAV supranta, kad Korėjos Respublikos teisinė sistema nenumato masinio duomenų perėmimo, o tik tikslinį telekomunikacijų duomenų perėmimą.[77] Europos Komisija patvirtino šį supratimą.

152. Atsižvelgiant į tai, pirmiau minėti EŽTT sprendimai, atitinkantys ESTT praktiką[78] ir ankstesnę EŽTT praktiką[79], dar kartą parodo visapusiškos nepriklausomų priežiūros institucijų vykdomos priežiūros svarbą. EDAV pabrėžia, kad nepriklausoma priežiūra visuose vyriausybės prieigos prie duomenų proceso etapuose teisėsaugos ir nacionalinio saugumo tikslais yra svarbi apsauga nuo savavališkų stebėjimo priemonių, taigi ir užtikrina tinkamo duomenų apsaugos lygio įvertinimą. Priežiūros institucijų nepriklausomumo garantija, kaip apibrėžta Chartijos 8 straipsnio 3 dalyje, skirta veiksmingai ir patikimai stebėsenai, kaip laikomasi asmenų apsaugos tvarkant asmens duomenis taisyklių, užtikrinti. Tai ypač taikytina tomis aplinkybėmis, kai dėl slapto stebėjimo pobūdžio asmeniui neleidžiama siekti peržiūros arba tiesiogiai dalyvauti bet kokioje peržiūros procedūroje prieš vykdant stebėjimo priemonę arba jos vykdymo metu.

153. Išankstinio nepriklausomo patvirtinimo nebuvimas pats savaime negali būti laikomas esminiu Korėjos teisės trūkumu vertinant iš esmės lygiavertį duomenų apsaugos lygį. Tinkamumo vertinimas vėlgi priklauso nuo visų atvejo aplinkybių, ypač nuo *ex post* priežiūros veiksmingumo ir teisės kreiptis į teismą, kaip numatyta Korėjos teisinėje sistemoje (žr. tolesnius 4.7 ir 4.8 skyrius).

4.4. Savanoriškas informacijos atskleidimas

154. Remiantis TBA 83 straipsnio 3 dalimi, telekomunikacijų paslaugų teikėjai nacionalinio saugumo institucijoms ir teisėsaugos institucijoms paprašius gali savanoriškai perduoti vadinamuosius abonento duomenis[80]. Nors EDAV pažymi, kad atvejai, susiję su asmens duomenimis, kurie buvo perduoti iš EEE į Korėją, greičiausiai bus reti, juos vis tiek reikia išanalizuoti, kad būtų galima įvertinti duomenų apsaugos lygį, kaip jau minėta pirmiau.

---

[75] Žr. 2020 m. spalio 6 d. ESTT sprendimo *La Quadrature du Net ir kiti* sujungtose bylose C-511/18, C-512/18 ir C-520/18, 124 punktą.

[76] Žr. 2021 m. gegužės 25 d. EŽTT sprendimo *Big Brother Watch ir kiti prieš UK*, ECLI:CE:ECHR:2021:0525JUD005817013, 351 punktą: „Masiniam perėmimui iš pradžių turėtų būti suteiktas nepriklausomas leidimas“, „masinį perėmimą turėtų leisti atlikti nepriklausoma institucija, tai yra institucija, nepriklausoma nuo vykdomosios valdžios“.

[77] Tik II priedo 3.2 skyriuje pateikiama aiški deklaracija nacionalinio saugumo tikslais, kai nurodoma, kad apribojimai ir apsaugos priemonės „*užtikrina, kad informacija būtų renkama ir apdorojama tik tiek, kiek tikrai būtina teisėtam tikslui pasiekti. Tai neapima bet kokio masinio ir besąlygiško asmens duomenų rinkimo nacionalinio saugumo tikslais*“.

[78] Žr., pavyzdžiui, ESTT sprendimą *Tele2 Sverige AB ir kiti* sujungtose bylose C-203/15 ir C-698/15, ECLI:EU:C:2016:970.

[79] Žr., pavyzdžiui, 2015 m. gruodžio 4 d. EŽTT sprendimą *Case of Roman Zakharov prieš Russia*, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Susiję duomenų rinkiniai apimtų: vardą ir pavardę, gyventojo registracijos numerį, adresą ir telefono numerį, datas, kada vartotojai užsisakė ar nutraukė savo abonementą, taip pat vartotojo identifikavimo kodus (naudojamus teisėtam kompiuterių sistemų ar ryšių tinklų naudotojui nustatyti).

155. EDAV supranta, kad tokiais atvejais yra taikomos PIPA duomenų apsaugos priemonės ir valdžios institucijos bei telekomunikacijų paslaugų teikėjai turi laikytis šių reikalavimų[81] ir kad abu gali būti laikomi atsakingais už bet kokius atitinkamų duomenų subjektų teisių ir laisvių pažeidimus[82] Be to, EDAV supranta, kad nėra reikalaujama, jog telekomunikacijų paslaugų teikėjai vykdytų tokius prašymus.

156. Tačiau kalbant apie koncepciją, pagal kurią nacionalinės valdžios institucijos gali naudotis abonentų duomenimis teisėsaugos tikslais ir visų pirma nacionalinio saugumo tikslais, telekomunikacijų verslo subjektams savanoriškai atskleidžiant duomenis, kyla susirūpinimas dėl padidėjusios rizikos duomenų subjektų teisėms ir laisvėms, ypač atsižvelgiant į jų teisę į informaciją.

157. Pagal PIPA 58 straipsnio 1 dalies 2 punktą, III–VII skyrių nuostatos netaikomos jokiems prašomiems pateikti asmens duomenims, susijusiems su nacionaliniu saugumu. Pavyzdžiui, šiuo atžvilgiu tokiems prašymams netaikomos PIPA 18 straipsnio (asmens informacijos netikslinio naudojimo ir teikimo apribojimas) ir 20 straipsnio (pranešimas apie asmens duomenų, surinktų iš trečiųjų šalių, šaltinius ir kt.) nuostatos. Tais atvejais, kai prašymą pateikia nacionalinio saugumo institucija, viena vertus, kyla klausimas, ar pagal 58 straipsnio 1 dalies 2 punktą taip pat draudžiama taikyti PIPA ir telekomunikacijų paslaugų teikėjams. Kita vertus, kyla klausimas, ar PIPA 20 straipsnio taikymo išimtis tokiais atvejais taip pat taikoma atitinkamai I priedo 3 skyriaus nuostatai (pranešimas apie duomenis, kai asmens duomenys nebuvo gauti iš duomenų subjekto (Įstatymo 20 straipsnis)). Jei taip būtų ir jei 58 straipsnio 1 dalies 2 punkte taip pat būtų kalbama apie telekomunikacijų paslaugų teikėjus, remiantis turima informacija kiltų rizika, kad nebūtų teisinės pareigos informuoti duomenų subjektus apie savanorišką duomenų atskleidimą.

158. Todėl EDAV yra susirūpinusi, kad informacijos reikalavimai gali tapti neveiksmingi ir todėl duomenų subjektams bus žymiai sunkiau ginti savo teises į duomenų apsaugą, ypač dėl sprendimų apskundimo teismine tvarka. Šiuo atžvilgiu EDAV prašo Europos Komisijos patikslinti atitinkamų nuostatų taikymo sritį.

4.5. Tolesnis informacijos naudojimas

159. Tikslo apribojimo principas yra pagrindinis teisinis duomenų apsaugos reikalavimas. Pagal jį reikalaujama, kad asmens duomenys būtų renkami tik konkrečiais, aiškiais ir teisėtais tikslais ir nebūtų toliau tvarkomi su šiais tikslais nesuderinamu būdu. Be to, pagal ES teisę valdžios institucijoms leidžiama tvarkyti asmens duomenis siekiant užkirsti kelią baudžiamiesiems nusikaltimams, tirti ar patraukti baudžiamojon atsakomybėn, net jei šie duomenys iš pradžių buvo gauti kitais tikslais, jei šios institucijos turi teisinį pagrindą tvarkyti tokius duomenis pagal atitinkamą teisę ir tolesnis jų tvarkymas nėra neproporcingas[83].

160. Atsižvelgdama į tai, EDAV pažymi, kad Korėjos duomenų apsaugos sistemoje numatytos apsaugos priemonės ir apribojimai, susiję su tolesniu informacijos, surinktos teisėsaugos ir nacionalinio saugumo tikslais, naudojimu, pvz., PIPA 3 straipsnio 1 dalies 2 punkte pateiktas tikslo apribojimo principas, panašūs į tuos, kurie numatyti ES teisėje.

4.6. Tolesnis perdavimas ir dalijimasis žvalgybos informacija

161. BDAR 44 straipsnyje nustatyta, kad asmens duomenų perdavimas ir tolesnis perdavimas gali būti vykdomas tik tuo atveju, jei nepažeidžiamas BDAR garantuojamas apsaugos lygis. Taigi, iš EEE į Korėją perduodamų asmens duomenų užtikrinamam apsaugos lygiui neturi pakenkti tolesnis perdavimas

[81] Žr. sprendimų projekto 164 ir 194 konstatuojamąsias dalis.
[82] Žr. sprendimo projekto 166 konstatuojamąją dalį.
[83] Žr. Teisėsaugos direktyvos 4 straipsnio 2 dalį.

gavėjams trečiojoje šalyje, t. y. tolesnis perdavimas turėtų būti leidžiamas tik tada, kai yra ir toliau užtikrinamas apsaugos lygis, iš esmės prilygstantis numatytam pagal ES teisę lygiui. Todėl vertinant, ar trečioji šalis užtikrina tinkamą duomenų apsaugos lygį, reikia atsižvelgti į šalies teisinį tolesnio perdavimo pagrindą. Tai neginčijama ir atitinka tiek Europos Komisijos[84], tiek EDAV požiūrį.

162. Šiomis aplinkybėmis EDPB atkreipia dėmesį į tai, kad EŽTT savo neseniai priimtuose sprendimuose *Big Brother Watch ir kt. prieš UK* ir *Centrum för Rättvisa prieš Švediją* pateikė gaires[85] dėl duomenų apsaugos atsargumo priemonių, kurių turi būti laikomasi susitariančiosiose valstybėse perduodant asmens duomenis kitoms šalims teisėsaugos ir nacionalinio saugumo tikslais masinio duomenų rinkimo atveju: „*Visų pirma, aplinkybės, kuriomis toks perdavimas gali įvykti, turi būti aiškiai išdėstytos nacionalinėje teisėje. Antra, perduodanti valstybė turi užtikrinti, kad gaunančioji valstybė, tvarkydama duomenis, turėtų apsaugos priemones, kuriomis galima užkirsti kelią piktnaudžiavimui ir neproporcingam kišimuisi. Gaunančioji valstybė visų pirma turi garantuoti saugų informacijos saugojimą ir apriboti jos tolesnį atskleidimą. […] Trečia, tuomet, kai bus aišku, kad yra perduodama informacija, dėl kurios reikia laikytis ypatingo konfidencialumo, pavyzdžiui, konfidenciali žurnalistinė medžiaga, bus būtinos sustiprintos apsaugos priemonės*.“[86]

163. Taikydamas šiuos standartus, EŽTT sprendime *Centrum för Rättvisa prieš Švediją* nustatė, kad tai, jog perėmimo tvarkoje nėra jokio aiškaus teisinio reikalavimo įvertinti dalijimosi žvalgybos informacija būtinumą ir proporcingumą, atsižvelgiant į jo galimą poveikį teisei į privatumą, yra EŽTK 8 straipsnio pažeidimas. EŽTT kritikavo, kad, dėl teisės bendrumo lygio, perimta informacija paprastai galėtų būti siunčiama į užsienį, kai laikoma, kad tai daroma užtikrinant nacionalinius interesus, nepriklausomai nuo to, ar gavėjas užsienyje suteikia tinkamą minimalų apsaugos lygį[87].

164. Pripažindama, kad pagal Pietų Korėjos teisinę sistemą neleidžiamas masinis duomenų perėmimas, bet atsižvelgdama į EŽTT praktikos padarinius, kaip nurodyta pirmiau, EDAV mano, kad, vertinant, ar teisinėje tolesnio perdavimo į trečiąją šalį sistemoje nustatyti tinkami duomenų apsaugos standartai, be reikalavimų, kylančių iš ES teisės, kaip aiškino ESTT, laikymosi, reikėtų atsižvelgti į EŽTT argumentus.

4.6.1. Teisinė sistema, taikoma teisėsaugos institucijų vykdomam tolesniam duomenų perdavimui

165. Kalbant apie tolesnį kompetentingų institucijų vykdomą duomenų perdavimą teisėsaugos tikslais, EDAV iš Europos Komisijos paaiškinimų supranta, kad yra taikomas sprendimo projekto I priedo 2 skyrius dėl duomenų tolesnio perdavimo apribojimo, įskaitant atvejus, kai duomenų perdavimas atliekamas remiantis kitu nei PIPA įstatymu. Remiantis šia taisykle, „*jei asmens duomenys yra teikiami trečiajai šaliai užsienyje, gali būti neužtikrinta tokio lygio jų apsauga, kurią garantuoja Korėjos Asmens duomenų apsaugos įstatymas dėl skirtingų šalių asmens duomenų apsaugos sistemų skirtumų. Atitinkamai tokie atvejai bus laikomi šio įstatymo 17 straipsnio 4 dalyje nurodytais „atvejais, kai duomenų subjektas gali patirti nepalankias sąlygas“ arba „atvejais, kai nesąžiningai pažeidžiamas duomenų subjekto ar trečiosios šalies interesas“, minimais šio įstatymo 18 straipsnio 2 dalyje ir to paties įstatymo vykdymo dekreto 14 straipsnio 2 dalyje. Todėl, kad įvykdytų šių nuostatų reikalavimus, asmens duomenų valdytojas ir trečioji šalis turi aiškiai užtikrinti įstatymui lygiavertį apsaugos lygį,*

[84] Žr. sprendimo projekto 84 konstatuojamąją dalį ir tolesnes dalis.

[85] Šie elementai buvo nustatyti sprendimų *Big Brother Watch* ir *Centrum för Rättvisa*, susijusių su masinio duomenų perėmimo tvarka, atveju. Reikalavimas dėl atsargumo priemonių, kurių reikia imtis perduodant informaciją kitoms šalims, jau buvo EŽTT parengtų kriterijų, susijusių su tiksliniu perėmimu, dalis ir EŽTT toliau jo nepatikslino (žr. *Big Brother Watch ir kiti prieš UK*, 335 ir 362 punktus).

[86] 2021 m. gegužės 25 d. EŽTT sprendimas *Big Brother Watch ir kiti prieš UK*, ECLI:CE:ECHR:2021:0525JUD005817013, 362 punktas.

[87] Žr. 2021 m. gegužės 25 d. EŽTT sprendimo *Centrum för Rättvisa prieš Švediją*, ECLI:CE:ECHR:2021:0525JUD003525208, 326 punktą.

įskaitant garantiją, kad duomenų subjektas galės naudotis savo teisėmis teisiškai privalomuose dokumentuose, pvz., sutartyse, netgi po to, kai asmens duomenys perduodami į užsienį[88]*."*

166. EDAV palankiai vertina šią nuostatą, kuri, darant prielaidą, kad duomenų apsaugos lygis Korėjoje yra tinkamas šiam tikslui, užtikrina tokį apsaugos lygio tęstinumą, kuris iš esmės garantuojamas tolesniam duomenų perdavimui pagal ES teisę. Komisija patvirtino, kad EDAV supratimas, būtent, kad šis I priedo skyrius yra taikomas visam tolesniam kompetentingų institucijų vykdomam duomenų perdavimui teisėsaugos tikslais, yra teisingas. Tačiau EDAV atkreipia dėmesį į tai, kad turi būti užtikrinta, jog šiuo reglamentu būtų nustatomas nuolatinis apsaugos lygis praktikoje, nes gali kilti neaiškumų, kokios sutarčių apsaugos priemonės ir įpareigojimai ar kiti panašūs mechanizmai gali būti naudojami siekiant tokio lygio apsaugos tvarkymo teisėsaugos tikslais atveju. Šiuo atžvilgiu reikėtų papildomai nurodyti, kad, pavyzdžiui, asmens duomenimis galima dalytis tik su atitinkamomis trečiosios šalies kompetentingomis institucijomis.

167. Atsižvelgdama į pirmiau pateiktą paaiškinimą dėl to, ar KOFIU yra įtrauktas į sprendimo projektą, EDAV pažymi, kad oficiali atstovybė dėl vyriausybės prieigos[89] paaiškino, jog pagal ARUSFTI 8 straipsnio 1 dalį KOFIU narys gali suteikti užsienio finansų žvalgybos tarnyboms nurodytą informaciją apie finansinius sandorius, jei manoma, kad tai būtina ARUSFTI tikslui pasiekti[90] Pačiame ARUSFTI 8 straipsnyje nenumatoma pareiga nustatyti, ar užsienio šalis suteikia tinkamas duomenų apsaugos priemones ir jas užtikrinti. II priede šiuo atžvilgiu nėra nuorodos į naują I priedo skyrių. Todėl EDAV ragina Europos Komisiją paaiškinti atitinkamo I priedo skyriaus, susijusio su tolesnio duomenų pervedimo apribojimu, ir tolesnio pervedimo teisinio pagrindo sąsają pagal ARUSFTI.

4.6.2. Teisinė sistema, taikoma tolesniam duomenų perdavimui nacionalinio saugumo tikslais

168. Sprendimo projekte nėra jokios informacijos apie tolesnio perdavimo teisinį pagrindą nacionalinio saugumo srityje. Todėl EDAV supranta, kad, skirtingai nei teisėsaugos tikslais, I priedo 2 skyrius netaikomas tolesniam duomenų perdavimui nacionalinio saugumo tikslais. PIPA 17 ir 18 straipsniai, kuriems taikomas atitinkamas I priedo skyrius, yra PIPA III skyriuje, kuris savo ruožtu netaikomas asmens duomenų tvarkymui nacionalinio saugumo tikslais (PIPA 58 straipsnio 1 dalis).

169. Tačiau EDAV daro prielaidą, kad Korėjai gali prireikti perduoti ir ji perduoda asmens duomenis užsienio žvalgybos tarnyboms nacionalinio saugumo tikslais, pvz., siekiant bendradarbiauti kovojant su tarpvalstybinėmis grėsmėmis nacionaliniam saugumui, įspėti užsienio vyriausybes apie tokias grėsmes ar prašyti jų pagalbos joms atpažinti.

170. EDAV suprato, kad, Europos Komisijos nuomone, tolesnis duomenų perdavimas Korėjos teisėje yra pakankamai reglamentuojamas apsaugos priemonėmis, kurios nustatytos visa apimančioje konstitucinėje sistemoje, visų pirma būtinumo ir proporcingumo principais, taip pat PIPA reglamentuojamais pagrindiniais duomenų apsaugos principais, pvz., tvarkymo teisėtumo ir sąžiningumo, tikslo apribojimo, duomenų kiekio mažinimo, saugumo ir bendros pareigos užkirsti kelią piktnaudžiavimui asmens duomenimis ir netinkamam jų naudojimui.

171. EDAV pripažįsta ir patvirtina bendrą šių pagrindinių (duomenų apsaugos) principų taikomumą, tačiau jai kyla susirūpinimas dėl to, kad šios apsaugos priemonės yra labai bendro pobūdžio ir teisiniame pagrinde nėra konkrečiai nurodomos ar nagrinėjamos konkrečios aplinkybės ir sąlygos, susijusios su

[88] Sprendimo projektas, I priedas, p. 7.
[89] Žr. sprendimo projekto II priedą.
[90] Žr. sprendimo projekto II priedo 2.2.3.2 skyrių. Nors toks keitimasis informacija gali būti vykdomas tik su sąlyga, kad užsienio tarnyba negali naudoti informacijos jokiais kitais tikslais, išskyrus pradinį jos atskleidimo tikslą, ir ypač – ne nusikalstamų veikų tyrimui ar teismui (ARUSFTI 8 straipsnio 2 dalis), KOFIU narys, gavęs užsienio šalies prašymą, gali duoti sutikimą, kad tokie duomenys būtų naudojami atliekant nusikalstamų veikų tyrimus ar nagrinėjant bylas dėl baudžiamųjų nusikaltimų, gavus išankstinį teisingumo ministro sutikimą (ARUSFTI 8 straipsnio 3 dalis).

tolesniu EEE perduotų duomenų perdavimu nacionalinio saugumo tikslais. Nors šie bendrieji ir visa apimantys principai yra plačiai taikomi, EDAV abejoja, ar galima laikyti, kad jie atitinka aiškių ir tikslių taisyklių kriterijus ir ar jais pakankamai įtvirtintos veiksmingos ir vykdytinos apsaugos priemonės. Labai svarbu, kad būtų aiškios ir išsamios taisyklės, ypač kai vyriausybės prieiga prie asmens duomenų ir jų tvarkymas vykdomas slaptai, o išvados, kurias galima padaryti iš duomenų, yra ypač griežtos. Siekiant asmeniui suteikti tinkamą apsaugą, įstatyme turėtų būti pakankamai aiškiai nurodytas kompetentingoms institucijoms suteiktos bet kurios diskrecijos mastas ir jos naudojimo būdas. Sprendime *Schrems II* ESTT primena, kad pačiame teisiniame pagrinde, kuriuo remiantis leidžiama kištis į pagrindines teises, siekiant laikytis būtinumo ir proporcingumo principų reikalavimų, turi būti apibrėžtas naudojimosi šia teise apribojimo mastas ir nustatytos aiškios ir tikslios taisyklės, reglamentuojančios nagrinėjamos priemonės apimtį bei taikymą, ir nustatytos minimalios apsaugos priemonės[91]. Todėl EDAV yra susirūpinusi dėl to, kad nepakanka, jog tokios apsaugos priemonės būtų bendrai įtvirtintos aukštesnės galios teisės normose, jei į patį atitinkamą teisinį pagrindą nėra konkrečiai įtraukta, pvz., proporcingumo sąvoka.

172. Šį susirūpinimą patvirtina pirmiau minėtas EŽTT sprendimas, kuriame teismas nustatė, kad bendra taisyklė, be jokio aiškaus reikalavimo įvertinti būtinumą ir proporcingumą ar apsvarstyti privatumo problemas, pagal EŽTK 8 straipsnį nėra suderinama su teise į privatumą. Šiuo atžvilgiu EDAV pažymi, kad minėtos bylos teisėje (taip pat Korėjos teisėje) egzistuoja pagrindiniai (konstitucijoje garantuoti) būtinumo ir proporcingumo principai, pvz., remiantis Chartiją ir prisijungiant prie EŽTK.

173. EDAV ragina Europos Komisiją paaiškinti teisinį pagrindą dėl to, kaip, kokiu mastu ir kokiomis konkrečiomis sąlygomis žvalgybos tarnybos privalo atsižvelgti į privatumo problemas ir duomenų apsaugos priemones prieš atskleisdamos asmens duomenis užsienio partneriams nacionalinio saugumo tikslais. Tuo atveju, jei šis įpareigojimas kyla tiesiogiai iš konstitucinių principų, Europos Komisija turėtų išsamiau įvertinti atitinkamo įstatymo tikslumo ir aiškumo reikalavimus ir patvirtinti, kad bendrieji konstituciniai ir duomenų apsaugos principai yra tinkamai taikomi ir įgyvendinami.

4.6.3. Tarptautiniai susitarimai

174. EDAV pažymi, kad Europos Komisija, atlikdama tinkamumo vertinimą neatsižvelgė į tai, ar tarp Korėjos ir trečiųjų šalių ar tarptautinių organizacijų yra sudaryti tarptautiniai susitarimai, kuriuose gali būti numatytos konkrečios nuostatos dėl teisėsaugos ir (arba) žvalgybos tarnybų tarptautinio asmens duomenų perdavimo trečiosioms šalims. EDAV mano, kad dvišalių ar daugiašalių susitarimų sudarymas su trečiosiomis šalimis teisėsaugos ar žvalgybos bendradarbiavimo tikslais gali turėti įtakos įvertintai Korėjos duomenų apsaugos teisinei sistemai.

175. Todėl EDAV ragina Europos Komisiją išsiaiškinti, ar tokie susitarimai yra, kokiomis sąlygomis jie gali būti sudaryti ir įvertinti, ar tarptautinių susitarimų nuostatos gali turėti įtakos apsaugos lygiui, kuris suteikiamas iš EEE į Korėją perduodamiems asmens duomenims pagal teisės aktų sistemą ir praktiką, susijusią su informacijos atskleidimu užsienyje teisėsaugos ir nacionalinio saugumo tikslais.

4.7. Priežiūra

176. EDAV pažymi, kad baudžiamosios teisėsaugos ir nacionalinių saugumo institucijų priežiūrą užtikrina įvairių vidaus ir išorės institucijų grupė.

177. Šiomis aplinkybėmis reikia pažymėti, kad ESTT ne kartą pabrėžė nepriklausomos priežiūros, kaip esminio fizinių asmenų apsaugos komponento tvarkant jų asmens duomenis, poreikį. Nepriklausomumo sąvoka apima institucinio savarankiškumo, nurodymų nepaisymo ir materialinės nepriklausomybės sritis. Siekiant užtikrinti nuoseklią duomenų apsaugos teisės aktų stebėseną ir

[91] Žr. *Schrems II* 175 ir 180 punktus.

vykdymą, priežiūros institucijos turi naudotis veiksmingais įgaliojimais, įskaitant įgaliojimus koreguoti ir imtis taisomųjų veiksmų.

178. EDAV sutinka su Europos Komisijos išvada, kad, bendrai vertinant, galima laikyti, jog Korėja turi nepriklausomą ir veiksmingą priežiūros sistemą, nors kelios priežiūros sistemos įstaigos pačios neatitinka pirmiau minėtų reikalavimų. Pavyzdžiui, dauguma jų neturi vykdomųjų įgaliojimų ir apsiriboja tik rekomendacijų teikimu, pvz., Nacionalinė žmogaus teisių komisija arba Audito ir inspekcijų valdyba. Be to, dauguma atitinkamų viešųjų įstaigų nėra išimtinai duomenų apsaugos institucijos, bet paprastai joms yra pavestos ir kitos užduotys pagrindinių teisių apsaugos srityje.

179. Tačiau, remdamasi Europos Komisijos paaiškinimais, EDAV pažymi, kad teisėsaugos institucijų priežiūrą visapusiškai ir be išimties garantuoja PIPC. Todėl PIPC turi tyrimo, taisomuosius ir vykdymo įgaliojimus pagal PIPA ir kitus duomenų apsaugos įstatymus (pvz., CPPA), kurie taikomi visai teisėsaugos ir nacionalinių saugumo institucijų prieigos prie asmens duomenų sričiai.

180. Atsižvelgdama į tai, EDAV dar kartą norėtų pabrėžti, kad priežiūros institucijos, norėdamos vykdyti savo užduotis ir naudotis įgaliojimais, turi turėti pakankamai žmogiškųjų, techninių ir finansinių išteklių. Šiuo atžvilgiu, deja, trūksta bet kokios informacijos apie paskirtas priežiūros institucijas, ypač apie PIPC. Todėl EDAV pakartoja savo prašymą Europos Komisijai pateikti daugiau informacijos šiuo klausimu.

181. Apskritai EDAV norėtų pažymėti, kad sprendimo projekte beveik nėra teiginių, pavyzdžių ar skaičių, susijusių su priežiūros veikla, taip pat su priežiūros institucijų vykdomu duomenų apsaugos įstatymo teisiniu įgyvendinimu teisėsaugos ir nacionalinio saugumo srityje. Tai būtų naudinga vertinant priežiūros institucijų veiksmingumą.

1.8. Apskundimas teismine tvarka ir teisių gynimas

182. EDAV primena, kad tinkamam duomenų apsaugos lygiui užtikrinti labai svarbu, jog, esant neteisėtai prieigai prie duomenų ar jų tvarkymui, duomenų subjektams būtų suteikta išsamių taisomųjų veiksmų galimybė ir teisių gynimo priemonės. Šių teisių gynimo priemonių turi pakakti, kad duomenų subjektas galėtų susipažinti su apie jį saugomais duomenimis ir paprašyti juos ištaisyti arba ištrinti.

183. Atsižvelgiant į ESTT sprendimus *Schrems I* ir *Schrems II*, akivaizdu, kad, be teisės kreiptis į kompetentingas institucijas, veiksminga teisminė apsauga, kaip apibrėžta Chartijos 47 straipsnio 1 dalyje, yra labai svarbi darant prielaidą apie trečiosios šalies teisės tinkamumą.

184. EDAV pripažįsta, kad Korėja pagal PIPA nustatė įvairius būdus, kaip įgyvendinti asmenų teises susipažinti su duomenimis, juos išsaugoti, ištrinti ir sustabdyti jų tvarkymą. Tos teisės gali būti įgyvendintos kreipiantis į patį duomenų valdytoją arba pateikiant skundą PIPC arba kitoms priežiūros institucijoms, pvz., Nacionalinei žmogaus teisių komisijai. Be to, EDAV pripažįsta galimybę užginčyti duomenų valdytojų arba valdžios institucijų sprendimą, priimtą reaguojant į jų prašymą, remiantis Administracinių ieškinių įstatymu.

185. Be to, EDAV iš Europos Komisijos pateiktų paaiškinimų supranta, kad asmenys gali ginčyti teisėsaugos ir nacionalinio saugumo institucijų veiksmus kompetentinguose teismuose pagal Administracinių ieškinių įstatymą ir Konstitucinio Teismo įstatymą ir turi galimybę gauti žalos atlyginimą pagal Valstybės kompensacijos įstatymą[92].

186. Tačiau šiomis aplinkybėmis EDAV yra susirūpinusi dėl veiksmingo ES asmenų teisių gynimo nacionalinio saugumo atvejais, su kuriais nėra susijęs joks Korėjos pilietis. Kaip pažymėta 33 ir tolesnėse dalyse, nacionalinės saugumo institucijos neprivalo pranešti duomenų subjektams apie jų asmens duomenų rinkimą ir tvarkymą. Kadangi tokiais atvejais yra daug sunkiau gauti veiksmingą

[92] Žr. II priedo 3.2.4 punktą kartu su 2.4.3 punktu.

teisinę apsaugą, EDAV norėtų atkreipti dėmesį į tai, kad čia reikia tam tikrų teisinių apsaugos priemonių, jei tai susiję su iš EEE perduotais duomenimis. Pagal šias apsaugos priemones duomenų subjektams turi būti sudarytos galimybės teisiškai saugiu būdu imtis veiksmingų veiksmų neteisėto duomenų tvarkymo atžvilgiu, netrukdant pernelyg siauriems procedūriniams reikalavimams, pvz., kai nustatoma įrodinėjimo pareiga, kurios jie, nežinodami apie tvarkymą, negali įvykdyti. Be to, duomenų subjektams turi būti suteikta galimybė kreiptis į kompetentingą įstaigą, kuri atitinka CFR 47 straipsnio reikalavimus, t. y. kuri yra kompetentinga nustatyti, ar duomenys yra tvarkomi, patikrinti jų tvarkymo teisėtumą ir turėti vykdytinus taisomuosius įgaliojimus tuo atveju, jei duomenų tvarkymas yra neteisėtas. Šiomis aplinkybėmis vien tik teisės, pavyzdžiui, pateikti skundą NHRC, nepakaktų. Todėl EDAV ragina Komisiją išsamiau paaiškinti, kaip šie reikalavimai įgyvendinami procedūriniu ir esminiu požiūriu, pvz., ar duomenų subjektai gali kreiptis į PIPC, taip pat į teismą, nereikalaujant įrodyti atitinkamo duomenų tvarkymo.

187. Be to, EDAV pastebi, kad sprendimo projekte numatytas skundų perdavimo mechanizmas, t. y. ES asmenys gali pateikti skundą PIPC per savo nacionalinę duomenų apsaugos instituciją arba per EDAV. Tuomet, kai tyrimas bus baigtas, PIPC tuo pačiu kanalu nusiųs pranešimą asmeniui[93]. EDAV palankiai vertina pastangas palengvinti galimybę ginti savo teises Korėjos nacionalinio saugumo institucijų atžvilgiu. Tuo pat metu EDAV pasisako už tai, kad toks skundų perdavimo mechanizmas būtų nukreiptas per Europos nacionalines duomenų apsaugos institucijas, o ne per EDAV, nes jos yra kompetentingos ir labiau tinkamos atskiriems skundams nagrinėti.

188. Be to, EDAV pažymi galimą prieštaravimą dėl savanoriško informacijos atskleidimo. Viena vertus, sprendimo projekte teigiama, kad asmenims gali būti suteikta teisių gynimo galimybė, jei jų duomenys būtų atskleisti neteisėtai, gavus prašymą juos atskleisti savanoriškai, taip pat ir prašymą pateikusios teisėsaugos institucijos atžvilgiu[94]. Kita vertus, sprendimo projekte daroma nuoroda į tiesioginio poveikio reikalavimą, susijusį su asmens teise užginčyti valdžios institucijų veiksmus, ir pateikiami (tik) privalomo informacijos atskleidimo prašymai kaip pavyzdys tuo atveju, kai administracinis veiksmas laikomas darančiu tiesioginį poveikį teisei į privatumą[95]. Iš Europos Komisijos paaiškinimų EDAV supranta, kad faktiškai nėra teisių gynimo galimybių apribojimų prašymų savanoriškai atskleisti informaciją atžvilgiu, todėl prašo Europos Komisijos išsamiau tai paaiškinti sprendime, tiek teisėsaugos, tiek nacionalinio saugumo srityse (skirtingai nei skyriuje apie teisėsaugą, skyriuje apie savanorišką informacijos atskleidimą nacionalinio saugumo tikslais nėra jokio aiškaus pareiškimo dėl teisių gynimo šiomis aplinkybėmis).

[93] Žr. sprendimo projekto 205 konstatuojamąją dalį ir I priedą, p. 19.
[94] Žr. sprendimo projekto 166 konstatuojamąją dalį.
[95] Žr. Sprendimo projekto 181 konstatuojamąją dalį (teisėsauga) ir 208 ir 181 konstatuojamąsias dalis (nacionalinis saugumas).