Mišljenje 32/2021 o Nacrtu provedbene odluke Europske komisije u skladu s Uredbom (EU) 2016/679 o primjerenoj zaštiti osobnih podataka u Republici Koreji

Inačica 1.0

Doneseno 24. rujna 2021.

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

SADRŽAJ

1. SAŽETAK 4
1.1. Područja konvergencije 4
1.2. Izazovi 5
1.2.1. Općenito 5
1.2.2. Aspekti opće zaštite podataka 5
1.2.3. Pristup javnih tijela podatcima prenesenima u Republiku Koreju 6
1.3. Zaključak 7
2. UVOD 8
2.1. Korejski okvir za zaštitu podataka 8
2.2. Područje primjene procjene EDPB-a 8
2.3. Opći komentari i pitanja 9
2.3.1. Međunarodne obveze koje je usvojila Republika Koreja 9
2.3.2. Područje primjene odluke o primjerenosti 10
3. ASPEKTI OPĆE ZAŠTITE PODATAKA 10
3.1. Načela sadržaja 10
3.1.1. Pojmovi 11
3.1.2. Djelomična izuzeća predviđena PIPA-om 13
3.1.3. Razlozi za zakonitu i poštenu obradu u legitimne svrhe 14
3.1.4. Načelo ograničenja svrhe 15
3.1.5. Kvaliteta podataka i načelo proporcionalnosti 16
3.1.6. Načelo zadržavanja podataka 16
3.1.7. Načelo sigurnosti i povjerljivosti 17
3.1.8. Načelo transparentnosti 17
3.1.9. Posebne kategorije osobnih podataka 18
3.1.10. Prava na pristup, ispravak, brisanje i prigovor 18
3.1.11. Ograničenja daljnjih prijenosa 21
3.1.12. Izravni marketing 22
3.1.13. Automatizirano donošenje odluka i izrada profila 23
3.1.14. Odgovornost 24
3.2. Postupovni i provedbeni mehanizmi 24
3.2.1. Nadležno neovisno nadzorno tijelo 25
3.2.2. Postojanje sustava za zaštitu podataka koji jamči dobru razinu usklađenosti 25
3.2.3. Sustav za zaštitu podataka mora pružiti podršku i pomoć ispitanicima da ostvare svoja prava i odgovarajuće mehanizme pravne zaštite 26

4. PRISTUP I UPOTREBA OSOBNIH PODATAKA PRENESENIH IZ EUROPSKE UNIJE PREKO JAVNIH TIJELA U JUŽNU KOREJU 27

4.1. Opći okvir zaštite podataka u kontekstu pristupa vlade 27

4.2. Zaštita i zaštitne mjere podataka o potvrdi komunikacije u kontekstu pristupa vlade za potrebe izvršavanja zakonodavstva 28

4.3. Pristup korejskih javnih tijela komunikacijskim podatcima radi nacionalne sigurnosti . 29

4.3.1. Nema obveze obavještavanja pojedinaca o pristupu vlade komunikaciji između stranih državljana 29

4.3.2. Nema prethodnog neovisnog odobrenja za prikupljanje komunikacijskih podataka između stranih državljana 30

4.4. Dobrovoljna objavljivanja 31

4.5. Daljnja upotreba podataka 32

4.5. Daljnji prijenosi i razmjena obavještajnih podataka 32

4.6.1. Primjenjiv pravni okvir za daljnje prijenose tijela za izvršavanje zakonodavstva 33

4.6.2. Primjenjiv pravni okvir za daljnje prijenose radi nacionalne sigurnosti 34

4.6.3. Međunarodni sporazumi 35

4.7. Nadzor 35

4.8. Pravni lijek i sudska zaštita 36

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (s) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ („**Opća uredba o zaštiti podataka**"),

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru („**EGP**"), a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članak 12. i članak 22. Poslovnika,

DONIO JE SLJEDEĆE MIŠLJENJE:

1. SAŽETAK

1. Europska komisija pokrenula je 16. lipnja 2021. formalni postupak donošenja nacrta provedbene odluke („**nacrt odluke**") o primjerenoj zaštiti osobnih podataka u Republici Koreji na temelju Zakona o zaštiti osobnih podataka u skladu s Općom uredbom o zaštiti podataka[2].

2. Istoga dana Europska komisija zatražila je mišljenje Europskog odbora za zaštitu podataka („**EDPB**")[3]. EDPB-ova ocjena primjerenosti razine zaštite koja se pruža u Republici Koreji donesena je na temelju razmatranja samog nacrta odluke, kao i na temelju analize dokumentacije koju je Europska komisija stavila na raspolaganje[4].

3. EDPB se usredotočio na procjenu općih aspekata Opće uredbe o zaštiti podataka u nacrtu odluke i pristupa javnih tijela osobnim podatcima koji se iz EGP-a prenose za potrebe izvršavanja zakonodavstva i radi nacionalne sigurnosti, uključujući pravne lijekove dostupne pojedincima u EGP-u. EDPB je osim toga procijenio jesu li zaštitne mjere predviđene korejskim pravnim okvirom uspostavljene i učinkovite.

4. EDPB je u ovom radu kao glavne referentne materijale upotrebljavao Referentni dokument o primjerenosti Opće uredbe o zaštiti podataka[5] („**Referentni dokument o primjerenosti Opće uredbe o zaštiti podataka**") donesen u veljači 2018. te Preporuke EDPB-a 02/2020 o europskim temeljnim jamstvima za mjere nadzora[6].

1.1. Područja konvergencije

5. Glavni cilj EDPB-a jest Europskoj komisiji dati mišljenje o primjerenosti razine zaštite koja se pruža pojedincima čiji se osobni podatci prenose u Republiku Koreju. Važno je prepoznati da EDPB ne očekuje da korejski okvir za zaštitu podataka preslikava europsko pravo o zaštiti podataka.

[1] Upućivanja na „**države članice**" u ovom mišljenju treba tumačiti kao upućivanja na „države članice EGP-a".
[2] Vidjeti priopćenje za medije https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ibid.
[4] EDPB svoju analizu temelji na službenim prijevodima koje je pripremila korejska vlada.
[5] WP254, Referentni dokument o primjerenosti Opće uredbe o zaštiti podataka, 6. veljače 2018., (podržao EDPB, vidjeti https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Vidjeti Preporuke EDPB-a 02/2020 o europskim temeljnim jamstvima za mjere nadzora, donesene 10. studenoga 2020., https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

6. Međutim, EDPB podsjeća da članak 45. Opće uredbe o zaštiti podataka i sudska praksa Suda Europske unije (dalje u tekstu „**Sud Europske unije“)** zahtijevaju da zakonodavstvo treće zemlje bude usklađeno sa suštinom temeljnih načela sadržanih u Općoj uredbi o zaštiti podataka kako bi se smatralo da pruža primjerenu razinu zaštite. U tom kontekstu, korejski okvir za zaštitu podataka pokazuje brojne sličnosti s europskim okvirom za zaštitu podataka uz jedan zakonodavni akt koji obuhvaća i javni i privatni sektor a koji nadopunjuju zakonodavni akti specifični za pojedini sektor.

7. S obzirom na sadržaj, EDPB ističe glavna područja usklađenosti između okvira Opće uredbe o zaštiti podataka i korejskog okvira za zaštitu podataka za određene temeljne odredbe kao što su, primjerice koncepti (npr. „osobni podatci”, „obrada”, „ispitanik”), razlozi za zakonitu i poštenu obradu u legitimne svrhe, ograničavanje svrhe, kvaliteta i proporcionalnost podataka, zadržavanje, sigurnost i povjerljivost podataka, transparentnost i posebne kategorije podataka.

8. Uz prethodno navedeno, EDPB pozdravlja napore koje su uložili Europska komisija i korejske vlasti kako bi osigurali da Republika Koreja pruža jednaku razinu zaštite kao što je pruža Opća uredba o zaštiti podataka putem donošenja Obavijesti korejskog nadzornog tijela (nije primjenjivo samo za osobne podatke prenesene iz EGP-a u Koreju) radi popunjavanja svih praznina između Opće uredbe o zaštiti podataka i korejskog okvira za zaštitu podataka. EDPB u tom kontekstu želi naglasiti relevantnost ovih obavijesti za ocjenu primjerenosti Republike Koreje uz napomenu da primjerice pružaju relevantna objašnjenja o određenim važnim zaštitnim mjerama, među ostalim u vezi s opsegom primjene izuzeća iz PIPA-e za obradu pseudonimiziranih osobnih podataka za znanstvene, istraživačke i statističke svrhe, daljnje prijenose te pravila koja su primjenjiva u kontekstu pristupa javnih tijela podatcima.

1.2. Izazovi

9. Iako je EDPB prepoznao da su mnogi aspekti korejskog okvira za zaštitu podataka u načelu istovjetni europskom okviru za zaštitu podataka, zaključio je i da postoje određeni aspekti koje je potrebno detaljnije ispitati i objasniti. EDPB osobito smatra da se sljedeće stavke trebaju dodatno procijeniti kako bi se osiguralo da je postignuta u načelu istovjetna razina zaštite te da ih Europska unija treba pomno pratiti.

1.2.1. Općenito

10. EDPB ističe da Obavijest br. 2021-1 *ima status administrativnog pravila s pravnom obvezujućom snagom za voditelja obrade osobnih podataka u smislu da se svako kršenje Obavijesti može smatrati kršenjem relevantnih odredbi PIPA-e*[7]. Međutim, s obzirom na to da Obavijest sama po sebi ne uključuje dodatna pravila, nego objašnjenja na koji bi se način shvatila primjena zakonskog teksta PIPA-e te u smislu njegova općenitog značaja, posebice za odredbe o pseudonimizaciji prema PIPA-i, a za koje EDPB zaključuje da su predmet otvorenih sudskih predmeta, EDPB poziva Europsku komisiju na davanje dodatnih podataka o obvezujućem učinku, provedivosti i valjanosti Obavijesti br. 2021-1 te bi preporučio pažljivo praćenje iste u praksi, osobito njezine primjene, ne samo putem korejskog nadzornog tijela, nego i sudova, posebice ako se jednaka razina zaštite koju pruža korejski pravni okvir temelji na objašnjenjima koja su dana unutar iste.

1.2.2. Aspekti opće zaštite podataka

11. U vezi s područjem primjene odluke o primjerenosti, EDPB ističe da će pokrivati prijenose iz pravnog okvira EGP-a prema javnim i privatnim „voditeljima obrade osobnih podataka“ koji spadaju u opseg PIPA-e. EDPB shvaća da su subjekti u svojstvu izvršitelja obrade unutar značenja Opće uredbe o zaštiti podataka obuhvaćeni u ovom pojmu; međutim, kako bi se izbjegli nesporazumi, poziva Europsku

[7] Vidjeti Odjeljak I. Priloga I. nacrta odluke.

komisiju na pojašnjenje da će odluka o primjerenosti pokrivati i prijenose prema „izvršiteljima obrade“ u Koreji.

12. Važan aspekt koji bi EDPB htio istaknuti odnosi se na koncept pseudonimiziranih podataka u korejskom okviru za zaštitu podataka. Prema korejskom zakonu, odstupanja od broja relevantnih odredbi, uključujući onih o pravima pojedinih ispitanika i zadržavanje podataka, primjenjiva su za obradu pseudonimiziranih osobnih podataka. Prema Europskoj komisiji to je tako samo ako se pseudonimizirani osobni podatci obrađuju za potrebe statistike, znanstvenog istraživanja ili arhiviranja u javnom interesu. Međutim, ovu tvrdnju uglavnom potvrđuje Obavijest br. 2021-1 zbog čega su već spomenuta potreba za dodatnim podatcima i praćenje obvezujućeg učinka, provedivosti i valjanosti ove Obavijesti izuzetno relevantni u ovom kontekstu. Dodatno, EDPB poziva Europsku uniju da dodatno procijeni utjecaj pseudonimizacije prema korejskom zakonu i, što je najvažnije, na koji način može utjecati na temeljna prava i slobode ispitanika čiji se osobni podatci prenose u Republiku Koreju na temelju odluke o primjerenosti. EDPB posebice poziva Europsku komisiju da dodatno procijeni odstupanja iz članka 28. stavka 7. PIPA-e i članka 40. stavka 3. CIA-e te da pomno prati njihovu primjenu i relevantnu sudsku praksu kako bi osigurala da se prava ispitanika neopravdano ne ograničavaju kad se osobni podatci preneseni na temelju odluke o primjerenosti obrađuju u ove svrhe.

13. Nadalje, EDPB ističe da prema korejskom zakonu pravo na povlačenje privole postoji samo u određenim okolnostima i stoga poziva Europsku komisiju da dodatno procijeni utjecaj nedostatka općenitog prava na povlačenje privole te da pruži dodatna jamstva kako bi osigurala da je u svakom trenutku zajamčena temeljna razina zaštite podataka, gdje je to potrebno, uz objašnjenje uloge prava na obustavu na temelju PIPA-e u nedostatku općenitog prava na povlačenje privole.

14. S obzirom na daljnji prijenos, EDPB potvrđuje da će se općenito upotrebljavati informirana privola ispitanika kao osnova za prijenose podataka od voditelja obrade podataka u Koreji primatelju u trećoj zemlji te da Obavijest br. 2021-1 predviđa da pojedinci moraju biti obaviješteni o trećoj zemlji kojoj će biti pruženi njihovi podatci. Međutim, EDPB poziva Europsku komisiju da osigura da će informacije koje će biti pružene ispitaniku sadržavati i informacije o mogućim rizicima prijenosa koji nastaju zbog nedostatka odgovarajuće zaštite u trećoj zemlji te nedostatka odgovarajućih zaštitnih mjera. Nadalje, EDPB bi pozdravio jamstva u odluci o primjerenosti da se osobni podatci neće prenositi od korejskog voditelja obrade osobnih podataka u treću zemlju u svakoj situaciji u kojoj se prema Općoj uredbi o zaštiti podataka nije mogla pružiti valjana privola, npr. zbog neravnoteže moći.

15. S obzirom na imenovanje članova korejskog nadzornog tijela, EDPB bi pozvao Europsku komisiju da prati svaku promjenu koja bi mogla utjecati na neovisnost članova nadzornog tijela Južne Koreje, iako bi formalni postupak bio u skladu s Općom uredbom o zaštiti podataka te stoga zadovoljava test ekvivalentnosti s pravnim okvirom EGP-a.

16. Ponovno na temelju informacija koje je pružila Europska komisija, u proračunu ništa ne upućuje na posebne značajke osoblja dodijeljenog PIPC-u ni na financijska sredstva koja su im dodijeljena. EDPB bi stoga pozdravio dodatne informacije u nacrtu odluke o ovim dvjema relevantnim temama.

1.2.3. Pristup javnih tijela podatcima prenesenima u Republiku Koreju

17. EDPB je analizirao i korejski pravni okvir s obzirom na pristup vlade osobnim podatcima prenesenima iz EGP-a u Koreju za potrebe izvršavanja zakonodavstva i radi nacionalne sigurnosti. Uz priznavanje predstavljanja i jamstava koje pruža korejska vlast, kao što je navedeno u Prilogu II. nacrta odluke, EDPB je prepoznao brojne aspekte za koje je potrebno pojašnjenje ili koji izazivaju zabrinutost.

18. EDPB ističe da se odredbe PIPA-e primjenjuju bez ograničenja u području izvršavanja zakonodavstva. EDPB ujedno ističe da je obrada osobnih podataka u području nacionalne sigurnosti predmet ograničenijem skupu odredbi sadržanih u PIPA-i.

19. S obzirom na dobrovoljno objavljivanje osobnih podataka pružatelja telekomunikacijskih usluga prema nacionalnim sigurnosnim tijelima, EDPB je zabrinut da je nejasna veza između odjeljka 3. Priloga I. nacrta odluke, u kojem se navodi da pružatelji usluga načelno moraju obavijestiti dotičnog pojedinca kad se dobrovoljno slažu sa zahtjevom, te članka 58. stavka 1. točke 2. PIPA-e, tj. djelomični izuzetak radi potreba nacionalne sigurnosti. Zbog toga bi zahtjevi za podatcima mogli postati neučinkoviti te će se tako znatno otežati ostvarivanje prava na zaštitu podataka ispitanicima, posebice povezano sa sudskom zaštitom.

20. Iako nacrt odluke to ne definira izričito, EDPB iz objašnjenja koje je pružila Europska komisija zaključuje da korejski pravni okvir ne dozvoljava masovno presretanje telekomunikacijskih podataka. Stoga nedavna sudska praksa Europskog suda za ljudska prava („**ESLJP**“) o režimima masovnog presretanja neće biti izravno relevantna za procjenu razine zaštite podataka u Koreji.

21. Nacrt odluke ne sadržava nikakve informacije o pravnom okviru za daljnje prijenose u području nacionalne sigurnosti. Iako je EDPB zaključio da su, prema Europskoj komisiji, daljnji prijenosi radi potreba nacionalne sigurnosti dovoljno regulirani općim zaštitnim mjerama i načelima prema ustavnom okviru i PIPA-i, EDPB je zabrinut može li se to smatrati zadovoljavanjem zahtjeva preciznosti i jasnoće zakona te pruža li učinkovite i primjenjive zaštitne mjere. Zaštitne mjere na koje se Europska komisija poziva vrlo su općenite prirode i ne odnose se, pravno gledajući, na specifične okolnosti i uvjete pod kojima može doći do daljnjih prijenosa radi potreba nacionalne sigurnosti. U tom kontekstu EDPB ujedno ističe da Europska komisija nije uzela u obzir postojanje međunarodnih sporazuma sklopljenih između Republike Koreje i trećih zemalja ili međunarodnih organizacija koje mogu predvidjeti specifične odredbe za međunarodni prijenos osobnih podataka koje izvršava zakonodavstvo i/ili obavještajne službe trećim zemljama. EDPB smatra da će sklapanje bilateralnih ili multilateralnih sporazuma s trećim zemljama u svrhu izvršavanja zakonodavstva ili obavještajne suradnje vjerojatno utjecati korejski pravni okvir zaštite podataka kako je procijenjen.

22. EDPB ističe da je nadzor tijelâ kaznenog progona kao i nacionalnih sigurnosnih tijelâ osiguran kombinacijom različitih unutarnjih i vanjskih tijela, posebice PIPC-a koji ima dovoljne izvršne ovlasti.

23. Djelotvorni pravni lijekovi i pravna zaštita zahtijevaju da se ispitanici mogu obratiti nadležnom tijelu koje udovoljava zahtjevima članka 47. Povelje Europske unije o temeljnim pravima („**Povelja**“), tj. koje je nadležno za određivanja da se odvija obrada osobnih podataka, za potvrdu zakonitosti obrade te koje ima izvršne ovlasti za primjenu pravnog lijeka u slučaju nezakonite obrade osobnih podataka. S tim u vezi, EDPB od Europske komisije traži objašnjenje je li žalba PIPC-u ili postupak pred sudom predmet materijalnih i/ili proceduralnih zahtjeva kao što je teret dokaza te bi li pojedinci u EGP-u bili u mogućnosti zadovoljiti takve preduvjete.

1.3. Zaključak

24. EDPB smatra da je ova odluka o primjerenosti od iznimne važnosti uzimajući u obzir i da će, uz naglašene izuzetke u mišljenju, pokrivati prijenose u javnom i u privatnom sektoru.

25. EDPB pozdravlja napore koje su uložili Europska komisija i korejska tijela da bi uskladili korejski pravni okvir s europskim pravnim okvirom. Poboljšanja koja se namjeravaju uvesti putem Obavijesti br. 2021-1 radi premošćivanja razlika između ta dva pravna okvira iznimno su važna i dobro prihvaćena. Međutim, EDPB ističe da ostaju brojne zabrinutosti, uključujući one povezane s Obavijesti br. 2021-1, zajedno s potrebom za daljnjim pojašnjenjem drugih pitanja te preporučuje Europskoj komisiji da odgovori na te zabrinutosti i zahtjeve za pojašnjenje koje je iznio EDPB te da pruži dodatne informacije i objašnjenja za probleme navedene u ovom mišljenju.

2. UVOD

2.1. Korejski okvir za zaštitu podataka

26. Glavni zakonodavni akt kojim se regulira zaštita podataka u Republici Koreji je Zakon o zaštiti osobnih podataka (Zakon br. 10465 od 29. ožujka 2011., posljednji put izmijenjen Zakonom br. 16930 donesenim 4. veljače 2020., „**PIPA**“). Dopunjen je Provedbenim dekretom (Predsjednički dekret br. 23169 donesen 29. rujna 2011., posljednji put izmijenjen Predsjedničkim dekretom br. 30892 donesenim 4. kolovoza 2020., „Provedbeni dekret PIPA-e“) koji je zakonski obvezujuć i primjenjiv.

27. Dodatno uz PIPA-u, korejski okvir za zaštitu podataka uključuje regulativne „Obavijesti“ koje je izdalo korejsko nadzorno tijelo, Komisija za zaštitu osobnih podataka („**PIPC**“), koje donosi dodatna pravila o tumačenju i primjeni PIPA-e. Nedavno je PIPC usvojio Obavijest br. 2021-1 donesenu 21. siječnja 2021. (koja je izmijenila prethodnu Obavijest br. 2020-10 donesenu 1. rujna 2020., u nastavku teksta „**Obavijest br. 2021-1**“) o tumačenju, primjeni i provedbi određenih odredbi PIPA-e. Točnije, ova je Obavijest proizašla iz rasprava o primjerenosti između korejskih tijela i Europske komisije. Sadržava pojašnjenja o primjeni određenih odredbi PIPA-e, uključujući one koje se odnose na obradu osobnih podataka koji se prenose u Koreju na temelju predviđene odluke o primjerenosti[8] te *ima status administrativnog pravila s obvezujućom pravnom snagom za voditelja obrade podataka u smislu da se svako kršenje Obavijesti može smatrati kršenjem relevantnih odredbi PIPA-e*[9]. U tom kontekstu EDPB želi istaknuti da, bez obzira na to što se u nacrtu odluke navodi pod pojmom „Dodatna pravila“, Obavijest ne sadržava *zaista* dodatna pravila, nego objašnjenja čija je svrha pojašnjenje kako bi se zakonski tekst PIPA-e trebao razumjeti u primjeni, posebice s obzirom na podatke prenesene iz EGP-a. S tim u vezi EDPB bi preporučio pažljivo praćenje provedbe Obavijesti br. 2021-1 u praksi, posebice s obzirom na njezinu primjenu, ne samo od strane PIPC-a, nego i sudova, posebice ako se jednaka razina sigurnosti koju pruža korejski pravni okvir temelji na pojašnjenjima pruženima u Obavijesti br. 2021-1.

28. Drugi relevantni zakoni o zaštiti podataka u korejskom pravnom okviru određuju pravila za obradu osobnih podataka u specifičnim sektorima industrije kao što su:

- Zakon o upotrebi i zaštiti kreditnih podataka („**CIA**“) uključujući njegov Provedbeni dekret („**Provedbeni dekret CIA-e**“) koji određuju specifična pravila koja su primjenjiva za komercijalne operatere i specijalizirane subjekte (kao što su kreditne agencije, financijske ustanove) kad obrađuju osobne kreditne podatke kako bi odredili kreditnu sposobnost stranaka za financijske ili komercijalne transakcije;
- Zakon o promoviranju podataka i korištenju komunikacijske mreže i zaštiti podataka („**Zakon o mrežama**“);
- Zakon o zaštiti privatnosti komunikacija („**CCPA**“).

29. U području pristupa vlade, osim relevantnih odredbi sadržanih u PIPA-i i CPPA-u, EDPB je razmotrio druge zakonodavne akte, primjerice Zakon o kaznenom postupku („**CPA**“), Zakon o telekomunikacijskom poslovanju („**TBA**“), Zakon o prijavi i upotrebi određenih podataka o financijskim transakcijama („**ARUSFTI**“) i Zakon o nacionalnoj obavještajnoj službi („**NISA**“).

2.2. Područje primjene procjene EDPB-a

30. Nacrt odluke Europske komisije rezultat je procjene korejskog okvira za zaštitu podataka nakon čega su uslijedile rasprave s korejskom vladom. U skladu s člankom 70. stavkom 1. točke s Opće uredbe o

[8] Vidjeti Odjeljak I. Priloga I. nacrta odluke.
[9] Ibid.

zaštiti podataka, očekuje se da će EDPB pružiti neovisno mišljenje o zaključcima Europske komisije, identificirati nedostatke okvira primjerenosti, ako postoje, i nastojati dati prijedloge za njihovo rješavanje.

31. Kako bi se izbjeglo ponavljanje i radi podrške u procjeni korejskog pravnog okvira, EDPB je odabrao fokusirati se na specifične točke predstavljene u nacrtu odluke te pružiti svoju analizu i mišljenje o njemu, udaljavajući se od ponavljanja većine činjeničnih nalaza i procjena za koje EDPB nema indikacija za pretpostavku da zakon Republike Koreje ne bi bio u načelu istovjetan zakonu u EGP-u. Dodatno, u skladu sa sudskom praksom Suda Europske unije, vrlo važan dio analize pokriva pravni režim pristupa nacionalne sigurnosti osobnim podatcima prenesenim u Republiku Koreju te praksu njezina aparata nacionalne sigurnosti.

32. U svojoj je procjeni EDPB uzeo u obzir primjenjiv europski okvir za zaštitu podataka, uključujući članke 7., 8. i 47. Povelje, odnosno zaštitu prava na privatan i obiteljski život, pravno na zaštitu osobnih podataka i pravo na djelotvoran pravni lijek i pošteno suđenje te članak 8. Europske konvencije o ljudskim pravima koji štiti pravo na privatan i obiteljski život. Osim navedenog, EDPB je imao na umu zahtjeve Opće uredbe o zaštiti podataka kao i relevantnu sudsku praksu.

33. Cilj ovog postupka je davanje Europskoj komisiji mišljenja o ocjeni primjerenosti razine zaštite u Republici Koreji. Sud Europske unije dodatno je razradio pojam „odgovarajuće razine zaštite" koji je već postojao u sklopu Direktive 95/46. Važno je podsjetiti na standard koji je Sud Europske unije postavio u predmetu Schrems I, a to je da čak i ako „razina zaštite" u trećoj zemlji mora biti „u načelu istovjetna" onoj zajamčenoj u Europskoj uniji, „*sredstva koja su u tom pogledu dostupna u trećoj zemlji za osiguranje takve razine zaštite mogu se razlikovati od onih koja se koriste u EU-u*"[10]. Stoga cilj nije prenijeti europsko zakonodavstvo točku po točku, već utvrditi temeljne i ključne zahtjeve zakonodavstva koje se ispituje. Primjerenost se može postići kombinacijom prava ispitanika i obveza subjekata koji obrađuju osobne podatke ili koji kontroliraju takvu obradu i nadzor u sklopu neovisnih tijela. Međutim, pravila zaštite podataka učinkovita su samo ako su provediva i ako se prate u praksi. Stoga je potrebno razmotriti ne samo sadržaj pravila primjenjivih na osobne podatke prenesene u treću zemlju ili međunarodnu organizaciju, već i sustav koji je uspostavljen da bi se osigurala učinkovitost takvih pravila. Djelotvorni mehanizmi provedbe od iznimne su važnosti za učinkovitost pravila o zaštiti podataka[11].

2.3. Opći komentari i pitanja

2.3.1. Međunarodne obveze koje je usvojila Republika Koreja

34. Sukladno članku 45. stavku 2. točki (c) Opće uredbe o zaštiti podataka i referentnom dokumentu o primjerenosti Opće uredbe o zaštiti podataka[12], za vrijeme procjene primjerenosti razine zaštite treće zemlje, Europska komisija uzet će u obzir, među ostalim, međunarodne obveze koje je treća zemlja preuzela ili druge obveze koje proizlaze iz njezina sudjelovanja u multilateralnim ili regionalnim sustavima, osobito u vezi sa zaštitom osobnih podataka, kao i provedbom tih obveza.

35. Koreja je stranka u različitim međunarodnim sporazumima koji jamče pravo na privatnost, kao što su Međunarodni pakt o građanskim i političkim pravima (članak 17.), Konvencija o pravima osoba s invaliditetom (članak 22.) i Konvencija o pravima djeteta (članak 16.). Nadalje, Koreja kao član OECD-a pridržava se okvira privatnosti OECD-a, posebice smjernica kojima se uređuje zaštita privatnosti i prekogranični protoci osobnih podataka.

[10] C-362/14, *Maximilian Schrems protiv Data Protection Commissioner*, 6. listopada 2015., ECLI:EU:C:2015:650, st. 73.-74.
[11] WP254, str. 2.
[12] WP254, str. 2.

36. Osim toga, EDPB ističe sudjelovanje Koreje kao države promatrača u radu Savjetodavnog odbora Konvencije Vijeća Europe 108(+) iako još nije odlučila hoće li mu pristupiti.

2.3.2. Područje primjene odluke o primjerenosti

37. Prema Uvodnoj izjavi 5. nacrta odluke, Europska komisija zaključuje da Republika Koreja osigurava primjerenu razinu zaštite za osobne podatke prenesena od voditelja obrade ili izvršitelja obrade u Uniji voditeljima obrade osobnih podataka (npr. fizičke ili pravne osobe, organizacije, javne ustanove), a koje su obuhvaćene primjenom PIPA-e, uz izuzetak obrade osobnih podataka za misionarske aktivnosti religijskih organizacija i za nominaciju kandidata političkih stranaka[13] ili obradu osobnih kreditnih podataka u skladu s CIA-om voditelja obrade koji su predmet nadzora Komisije za financijske usluge.

38. EDPB ističe da će odluka o primjerenosti pokrivati prijenose iz pravnog okvira EGP-a prema javnim i privatnim „voditeljima obrade podataka“ koji pripadaju u opseg PIPA-e. EDPB shvaća da su subjekti u svojstvu voditelja obrade unutar značenja Opće uredbe o zaštiti podataka obuhvaćeni i pojmom „voditelj obrade osobnih podataka“ uzimajući u obzir da će se za njih jednako primjenjivati PIPA te da se primjenjuju specifične obveze kad voditelj obrade osobnih podataka („osoba koja zapošljava vanjskog suradnika“) angažira treću stranu za obradu osobnih podataka („vanjski suradnik“), međutim, kako bi se spriječili nesporazumi, EDPB poziva Europsku uniju da pojasni da će odluka o primjerenosti pokriti i prijenose „izvršiteljima obrade“ u Koreji te da razina zaštite osobnih podataka koji su prenesi iz EGP-a neće biti ugrožena ni u tim slučajevima.

39. Osim toga, uzimajući u obzir da odluka o primjerenosti pokriva i prijenose osobnih podataka između javnih tijela, EDPB zaključuje da će ovo pokriva i prijenose između nadzornih tijela za zaštitu podataka te, radi jasnoće, poziva Europsku komisiju da specifično odgovori na ovo pitanje.

40. Nadalje, s obzirom na subjekte koji su izuzeti iz opsega primjene odluke o primjerenosti, EDPB bi želio naglasiti da bi odluka o primjerenosti mogla imati koristi od jasnije identifikacije „komercijalnih organizacija“ koji su predmet nadzora PIPC-a (članak 45. stavak 3. CIA-e) tako da voditelji i izvršitelji obrade u EGP-u na jednostavan način mogu procijeniti je li i uvoznik obuhvaćen područjem primjene odluke o primjerenosti prije prijenosa podataka subjektima koji su obuhvaćeni područjem primjene CIA-e ili da barem budu obaviješteni o potrebi za procjenom ovog aspekta.

41. S obzirom na područje primjene odluke o primjerenosti, EDPB je iz dodatnih objašnjenja Europske komisije zaključio da je Korejska financijsko-obavještajna jedinica („**KOFIU**“), koja je ustanovljena unutar Komisije za financijske usluge i nadzire sprječavanje pranja novca i financiranja terorista u skladu s ARUSFTI-jem[14], također izuzeta iz područja primjene jer ima nadležnost jedino nad financijskim ustanovama koje nisu obuhvaćene nacrtom odlukom. Međutim, članak 1. stavak 2. točka (c) nacrta odluke iz svojeg područja primjene izuzima samo one voditelje obrade osobnih podataka koji su predmet nadzora Komisije za financijske usluge i obrađuju osobne kreditne podatke obuhvaćene CIA-om. Na temelju ovoga EDPB zahtijeva od Europske komisije pojašnjenje jesu li KOFIU i aktivnosti obrade podataka koje je poduzeo sam KOFIU obuhvaćene nacrtom odluke.

3. ASPEKTI OPĆE ZAŠTITE PODATAKA

3.1. Načela sadržaja

42. Poglavlje 3. Referentnog dokumenta o primjerenosti Opće uredbe o zaštiti podataka posvećeno je „Načelima sadržaja”. Sustav treće zemlje mora ih sadržavati kako bi se pružena razina zaštite smatrala u načelu istovjetnom onoj zajamčenoj zakonodavstvom EU-a.

[13] Za više konteksta vidjeti u nastavku odjeljak 3.1.2. ovog mišljenja.
[14] Vidjeti Prilog II., odjeljak 2.2.3.1.

43. Iako pravo na zaštitu osobnih podataka nije izričito utvrđeno u korejskom ustavu, prepoznato je kao osnovno pravo koje proizlazi iz ustavnih prava na ljudsko dostojanstvo i potragu za srećom (članak 10.), privatan život (članak 17.) i privatnost komunikacija (članak 18.). Ovo su potvrdili i Vrhovni sud i Ustavni sud, što je navedeno u nacrtu odluke Europske komisije[15]. EDPB uzima u obzir ovu potvrdu jer iz nje proizlazi da se zaštita podataka, kao osnovno pravo u skladu s člankom 37. korejskog ustava, „može ograničiti samo zakonom i, ako je potrebno, radi nacionalne sigurnosti ili održavanja zakona i reda ili radi javne sigurnosti“ i da „čak i kad su takva ograničenja nametnuta, ne mogu utjecati na suštinu slobode ili prava“.

44. Prema Europskoj komisiji[16], Ustavni je sud odlučio da temeljna prava vrijede i za strane državljane. Prema službenim predstavnicima korejske vlade[17], iako se sudska praksa do sada još nije suočila izričito s pravom na privatnost s državljanima koji nisu Koreanci, široko je prihvaćeno među stručnim krugovima da članci 12. – 22. Ustava označavaju „prava ljudskih bića“. Nadalje, Republika Koreja donijela je niz zakona u području zaštite podataka koji pružaju zaštitne mjere za sve pojedince, bez obzira na državljanstvo, kao što je PIPA. S obzirom na to, EDPB ističe da članak 6. stavak 2. Ustava govori da je status stranih državljana zajamčen prema međunarodnim propisima i sporazumima i spomenutoj sudskoj praksi u nacrtu odluke prema kojima „stranac“ može biti nositelj „osnovnih prava“. Uzimajući u obzir važnost prepoznavanja prava na zaštitu podataka za „strane državljane“, EDPB skreće pažnju Europske komisije na potrebu da se i dalje prati sudska praksa koja je povezana sa zaštitom podataka kao osnovnog prava priznatog i korejskim državljanima i svim ispitanicima kako bi se osiguralo da razina zaštite fizičkih osoba koju jamči Opća uredba o zaštiti podataka nije ugrožena kad se osobni podatci prenose u Koreju na temelju odluke o primjerenosti.

3.1.1. Pojmovi

45. Na temelju referentnog dokumenta o primjerenosti Opće uredbe o zaštiti podataka, pravni okvir treće zemlje treba sadržavati osnovne pojmove ili načela zaštite podataka. Iako ne moraju odražavati terminologiju Opće uredbe o zaštiti podataka, trebali bi odražavati pojmove sadržane u europskom pravu o zaštiti podataka te s njima biti usklađeni. Primjerice, Opća uredba o zaštiti podataka sadržava sljedeće važne pojmove: „osobni podaci”, „obrada osobnih podataka”, „voditelj obrade podataka”, „izvršitelj obrade podataka”, „primatelj” i „osjetljivi podaci”[18].

46. PIPA uključuje brojne definicije kao što su, među ostalim, one za „osobne podatke“, „obradu“ i „ispitanika“ koje su vrlo slične odgovarajućim pojmovima u Općoj uredbi o zaštiti podataka.

3.1.1.1. Pojam pseudonimiziranih podataka

47. Među definicijama utvrđenih PIPA-om, članak 2. stavak 1. PIPA-e definira posebice osobne podatke kao bilo koje podatke u nastavku koji se odnose na pojedince: (a) podatci kojima se identificira određeni pojedinac njegovim ili njezinim punim imenom, matičnim brojem stanovnika, slikom itd. i (b) podatci koji se, čak i kad samostalno ne identificiraju određenog pojedinca, mogu jednostavno kombinirati s drugim podatcima kako bi se utvrdio identitet određene osobe. U posljednjem će se slučaju postojanje jednostavnosti kombinacije odrediti racionalno uzimajući u obzir vrijeme, trošak, tehnologiju itd. koji su upotrijebljeni za identifikaciju pojedinca kao što je vjerojatnost da se ostali podatci mogu nabaviti.

48. Dodatno, u skladu s člankom 2. stavkom 1. točkom (c) PIPA-e, odnosno „pseudonimizirani podatci“ smatraju se osobnim podatcima. Pseudonimizirani podatci definirani su kao podatci pod prethodno

[15] Vidjeti Uvodnu izjavu 8. nacrta odluke i relevantnu sudsku praksu iz bilješke 10. nacrta odluke za koji postoje samo sažetci na engleskom jeziku.
[16] Vidjeti uvodnu izjavu 9. nacrta odluke.
[17] Odjeljak 1.1. Priloga II. nacrta odluke.
[18] WP254, str. 4.

navedenim stavkama (a) ili (b) koji su pseudonimizirani u skladu s podstavkom 1.-2. te stoga postaju nemogući za identifikaciju određenog pojedinca bez upotrebe ili kombinacije podataka za vraćanje na originalno stanje. Podatci koji su u potpunosti anonimizirani izuzeti su iz područja primjene PIPA-e. Prema članku 58. stavku 2. PIPA-e, zakon se ne odnosi na podatke kojima se više ne utvrđuje identitet određenog pojedinca kad se kombiniraju s drugim podatcima, racionalno uzimajući u obzir vrijeme, trošak, tehnologiju itd.

49. Europska komisija u Uvodnoj izjavi 17. svojeg nacrta odluke navodi da ovo odgovara materijalnom području primjene Opće uredbe o zaštiti podataka i njezinu pojmu „osobnih podataka", „pseudonimizaciji" i „anonimiziranim podatcima".

50. Međutim, prema članku 28. stavku 7. PIPA-e, članci 20., 21., 27., 34. stavak 1., od 35. do 37., članak 39. stavak 3., članak 39. stavak 4., članak 39. stavak 6. do 39. stavak 8. ne odnose se na pseudonimizirane osobne podatke.

51. U ovom nacrtu odluke Europska komisija navodi da je članak 28. stavak 7. PIPA-e primjenjiv samo na pseudonimizirane osobne podatke kad se obrađuju radi statistike, znanstvenog istraživanja ili arhiviranja od javnog interesa[19]. Međutim, to ne proizlazi izravno iz zakona, nego iz objašnjenja danih u Obavijesti br. 2021-1[20]. EDPB priznaje postojanje argumenta na temelju strukture i obrazloženja PIPA-e da bi se članak 28. stavak 2. PIPA-e trebao razumjeti i logički tumačiti kao da se odnosi i na članak 28. stavak 7. PIPA-e s obzirom na važnost Obavijesti br. 2021-1 u ocjeni Europske komisije o primjerenosti razine zaštite osobnih podataka u Republici Koreji, a kako bi se izbjegla svaka dvojba, EDPB poziva Europsku komisiju na davanje daljnjih informacija o obvezujućem učinku, provedivosti i valjanosti Obavijesti br. 2021-1 i na praćenje njezine primjene u ovom specifičnom kontekstu.

52. U ovom se kontekstu EDPB poziva na to da se na temelju Opće uredbe o zaštiti podataka pseudonimizacija shvaća kao preporučena sigurnosna mjera. Drugim riječima, na temelju Opće uredbe o zaštiti podataka pseudonimizirani podatci ostaju osobni podatci na koje se Opća uredba o zaštiti podataka u potpunosti primjenjuje. Na temelju prethodno navedenog, EDPB izražava zabrinutost da bi se razina zaštita Opće uredbe o zaštiti podataka za pseudonimizirane osobne podatke mogla smanjiti kad se osobni podatci prenose u Koreju. EDPB stoga poziva Europsku uniju da dodatno procijeni utjecaj pseudonimizacije prema PIPA-i i, što je najvažnije, na koji način može utjecati na temeljna prava i slobode ispitanika čiji bi se osobni podatci prenosili u Republiku Koreju na temelju odluke o primjerenosti. Stoga EDPB poziva Europsku komisiju na pružanje jamstava da se razina zaštite osobnih podataka ispitanika u EGP-u neće smanjiti nakon prijenosa u Republiku Koreju, čak i ako su osobni podatci koji se prenose pseudonimizirani.

3.1.1.2. *Pojam voditelja obrade osobnih podataka*

53. Članak 2. stavak 5. PIPA-e uključuje definiciju „voditelja obrade osobnih podataka" označavajući javnu ustanovu, pravnu osobu, organizaciju ili pojedinca itd. koji obrađuje osobne podatke izravno ili neizravno za upravljanje datotekama osobnih podataka „kao dijelom svojim aktivnosti". Međutim, u dodatnim zaštitnim mjerama navedenima u Obavijesti br. 2021-1, pojam voditelja obrade osobnih podataka definiran je kao javna ustanova, pravna osoba, organizacija, pojedinac itd. koji obrađuje osobne podatke izravno ili neizravno za upravljanje datotekama osobnih podatcima „u poslovne svrhe". Umjesto toga bilješka 272. nacrta odluke navodi sljedeće o pojmu voditelja obrade podataka: „Kao što je definirano člankom 2. PIPA-e, odnosno javna ustanova, pravna osoba, organizacija,

[19] Vidjeti, među ostalim, uvodnu izjavu 82. nacrta odluke.
[20] Odjeljak 4. Priloga I. nacrta odluke.

pojedinac itd. koji obrađuje osobne podatke izravno ili neizravno za upravljanje datotekama osobnih podataka „u službene ili poslovne svrhe“.“

54. EDPB priznaje da su ove nedosljednosti nastale zbog prijevoda originalnog teksta koji su dale korejske vlasti te poziva Europsku komisiju da redovito provjerava kvalitetu i točnost prijevoda. Međutim, EDPB naglašava činjenicu da je potrebno jasno razumijevanje svrha obrade obuhvaćenih materijalnim područjem primjene PIPA-e kako bi se mogla procijeniti načelna istovjetnost razine zaštite podataka korejskog pravnog okvira. Nadalje, EDPB u ovom kontekstu ističe da PIPA ne upotrebljava jednaku terminologiju Opće uredbe o zaštiti podataka povezano s pojmom „voditelja obrade“ i „izvršitelja obrade“ te poziva Europsku komisiju na razjašnjavanje točne definicije i opsega pojma „voditelja obrade osobnih podataka“ i da posebno razmotri obuhvaća li taj pojam izvršitelje obrade unutar značenja Opće uredbe o zaštiti podataka jer to izravno utječe na područje primjene odluke o primjerenosti[21].

3.1.2. Djelomična izuzeća predviđena PIPA-om

55. Članak 58. stavak 1. PIPA-e isključuje primjenu dijelova PIPA-e (odnosno članke 15. do 57.) s obzirom na četiri kategorije obrade osobnih podataka kako je opisano u nastavku. Izuzeća se posebice odnose na odredbe PIPA-e o posebnim razlozima obrade, određene obveze zaštite podataka, detaljna pravila za ostvarivanje pojedinačnih prava te pravila kojima se uređuje rješavanje sporova. Međutim, EDPB naglašava da se i dalje primjenjuju određene opće odredbe PIPA-e kao što su one koje se odnose na načela zaštite podataka (članak 3. PIPA-e) i pojedinačna prava (članak 4. PIPA-e). Dodatno, članak 58. stavak 4. PIPA-e navodi određene obveze tih četiriju kategorija obrade podataka.

56. Prvo, djelomično izuzeće obuhvaća osobne podatke prikupljene u skladu sa Zakonom o statistici za obradu putem javnih ustanova. Europska komisija u uvodnoj izjavi 27. svojeg nacrta odluke navodi da se, prema pojašnjenjima koja je dala korejska vlada, osobni podatci obrađeni u ovom kontekstu obično odnose na korejske državljane te da bi samo iznimno mogli obuhvaćati podatke o stranim državljanima, odnosno u slučaju statistike o dolasku i odlasku s državnog područja ili o stranima ulaganjima. Međutim, prema nacrtu odluke, čak i u ovim situacijama, podatci se obično ne prenose od voditelja/izvršitelja obrade u EGP, nego ih izravno prikupljaju javna tijela u Koreji.

57. EDPB priznaje mišljenje Europske komisije o iznimnoj primjeni Zakona o statistici na obradu osobnih podataka koji se prenose na temelju odluke o primjerenosti. Međutim, pozdravio bi dodatne informacije i jamstva o specifičnim zaštitnim mjerama koje bi se primjenjivale ako se osobni podatci preneseni iz EGP-a dalje prikupljaju prema Zakonu o statistici radi obrade putem javnih ustanova, posebice kad se to odnosi na ostvarivanje pojedinačnih prava ispitanika u skladu s člankom 89. stavkom 2. Opće uredbe o zaštiti podataka u dijelu kad takva prava vjerojatno neće onemogućiti ili ozbiljno ugroziti postignuća određenih svrha te takva odstupanja nisu potrebna za ostvarenje tih svrha.

58. U tom smislu, čini se da primjena članka 4. PIPA-e i na ovu vrstu obrade pruža jamstva, međutim, EDPB bi pozdravio dodatne informacije i pojašnjenja u odluci o primjerenosti glede specifičnih obveza, u skladu s člankom 58. stavkom 4. PIPA-e, povezanih s tim aktivnostima obrade, posebice koje se odnose na smanjenje količine podataka, ograničeno zadržavanje podataka, sigurnosne mjere i rješavanje žalbi.

59. Drugo, djelomično izuzeće obuhvaća osobne podatke prikupljene ili zatražene radi analize podataka povezanih s nacionalnom sigurnošću. EDPB je svjestan činjenice da u slučajevima nacionalne sigurnosti države imaju veliku slobodu odlučivanja koju prepoznaje Europski sud za ljudska prava. Osim toga, EDPB ističe da, u skladu s člankom 37. stavkom 2. korejskog ustava, svako ograničenje slobode i prava, primjerice, kad je to potrebno radi zaštite nacionalne sigurnosti, ne smije kršiti ključne aspekte tih sloboda ili prava. Nadalje, EDPB ističe zaštitne mjere u odjeljku 6. Obavijesti br. 2021-1 koje se odnose

[21] Vidjeti i prethodno navedenu t. 38.

na obradu osobnih podataka radi nacionalne sigurnosti, uključujući istraživanje povreda prava i provedbi. Međutim, EDPB u ovom kontekstu poziva Europsku komisiju na dodatno razjašnjavanje područja primjene izuzeća jer si postavlja pitanja jesu li sva izuzeća navedena u članku 58. stavku 1. točki 2. PIPA-e (Poglavlja III. do VII.) važna za rad obavještajnih službi te osiguravaju li istovjetnost s načelima nužnosti i proporcionalnosti. EDPB poglavito poziva Europsku komisiju na pružanje više pojašnjenja toga pod kojim bi se uvjetima obavještajne službe mogle pouzdati u izuzeća. EDPB smatra da je potrebno pomno pratiti utjecaj tih ograničenja u praksi, posebice na učinkovito ostvarivanje i provedbu prava ispitanika.

60. Treće, djelomično izuzeće odnosi se na „osobne podatke koji se obrađuju privremeno ako je to hitno nužno radi javne sigurnosti i zaštite, javnog zdravstva itd." Prema uvodnoj izjavi 29. nacrta odluke Europske komisije, ovu kategoriju PIPC strogo tumači i primjenjuje samo u hitnim situacijama koje zahtijevaju hitne radnje, primjerice, radi praćenja uzročnika infekcija ili radi zaštite i pomoći žrtvama prirodnih katastrofa.

61. EDPB ujedno naglašava da bi se svako odstupanje od razine zaštite za osobne podatke trebala strogo tumačiti. EDPB istodobno ističe da odredba nije strogo definirana i da se ne daje nepotpun popis primjera situacija u kojima bi se obrada osobnih podataka mogla smatrati „*hitno nužnom*". Primjerice, EDPB je zabrinut bi li međunarodni prijenos zdravstvenih podataka za vrijeme aktualne pandemije bolesti COVID-19 isto bio obuhvaćen područjem primjene ovog izuzeća. Uzimajući u obzir prethodna razmatranja, EDPB poziva Europsku komisiju na davanje dodatnih razjašnjenja o području primjene ovog izuzeća i na potpuno praćenje njezinog područja primjene i same primjene kako bi se osiguralo da ne vodi to toga da se razina zaštite osobnih podataka iz EGP-a smanjuje nakon prijenosa u Koreju na temelju oduke o primjerenosti.

62. Konačno, djelomično izuzeće odnosi se na osobne podatke prikupljene ili upotrijebljene za svrhe izvješćivanja medija, misionarske aktivnosti religijskih organizacija i nominaciju kandidata političkih stranaka[22]. S obzirom na obradu osobnih podataka putem medija radi novinarskih aktivnosti, Europska komisija u uvodnoj izjavi 31. svojeg nacrta odluke navodi da je ravnoteža između slobode govora i drugih prava, uključujući pravo na privatnost, propisana Zakonom o arbitraži i drugim pravnim lijekovima itd. za štete uzrokovane novinskim izvještajima (u nastavku teksta „**Zakon o medijima**") i predstavlja određene zaštitne mjere koje slijede iz Zakona o medijima. Međutim, EDPB bi pozvao Europsku uniju na potpuno praćenje ovog izuzeća i relevantne sudske prakse kako bi se osiguralo da je osigurana istovjetna razina zaštite podataka i u praksi u korejskom pravnom okviru.

3.1.3. Razlozi za zakonitu i poštenu obradu u legitimne svrhe

63. Prema referentnom dokumentu o primjerenosti Opće uredbe o zaštiti podataka i sukladno Općoj uredbi o zaštiti podataka, podatci se moraju obrađivati na zakonit, pravedan i legitiman način. Pravnu osnovu na temelju koje se osobni podatci mogu zakonito, pravedno i legitimno obrađivati potrebno je utvrditi na dovoljno jasan način. Europski okvir potvrđuje nekoliko takvih legitimnih razloga, uključujući, primjerice, odredbe nacionalnog prava, pristanak ispitanika, izvršavanje ugovornih obveza ili legitimni interes voditelja obrade podataka ili treće strane koji ne prevladava nad interesom pojedinca.

64. Pridržavanjem slične strukture Opće uredbe o zaštiti podataka, PIPA na početku prvo iznosi načelo zakonitosti, pravednosti i transparentnosti (članak 3. stavak 1. i 2. PIPA-e), određujući posebna pravila za kasniju primjenu (članci 15. do 19. PIPA-e). Članak 15. PIPA-e posebice uključuje katalog pravnih osnova na kojima bi voditelji obrade osobnih podataka mogli temeljiti prikupljanje osobnih podataka i upotrebljavati ih unutar područja prikupljanja svrha. Pravne osnove obuhvaćaju (1) informiranu

[22] U skladu s time, obrada osobnih podataka religijskih organizacija za svoje misionarske aktivnosti i obrada osobnih podataka političkih stranaka u kontekstu nominacije kandidata isto su isključene iz područja primjene odluke o primjerenosti. Vidjeti i gore navedenu t. 37. u odjeljku 2.3.2.

privolu ispitanika; (2) zakonsku ovlast ili nužnost za sukladnost sa zakonskom obvezom; (3) nužnost za provedbom obveza javne ustanove; (4) nužnost za provedbu ili izvršenje ugovora s ispitanikom; (5) nužnost zaštite života, tjelesnih ili imovinskih interesa ispitanika ili treće strane od neposredne opasnosti (a prethodna se privola nije mogla dobiti); (6) nužnost ostvarivanja opravdanog interesa voditelja obrade osobnih podataka, što je nadređeno onome ispitanika.

65. Dodatno, članak 17. PIPA-e navodi pravne osnove koje su primjenjive za dijeljenje osobnih podataka s trećom stranom koje uključuju (1) informiranu privolu ispitanika; (2) zakonsku ovlast ili nužnost za sukladnost sa zakonskom obvezom; (3) nužnost za provedbom obveza javne ustanove; i (4) nužnost zaštite života, tjelesnih ili imovinskih interesa ispitanika ili treće strane od neposredne opasnosti (a prethodna se privola nije mogla dobiti). Čak i ako nema privole ispitanika, dijeljenje osobnih podataka dozvoljeno je ako se provodi unutar opsega koji je razumno povezan sa svrhom radi koje su osobni podatci prvotno prikupljeni (članak 17. stavak 4. PIPA-e).

66. Članak 18. PIPA-e utvrđuje posebna pravila za upotrebu i dijeljenje osobnih podataka ako se provodi izvan opsega prvotne svrhe prikupljanja ili pružanja. Među ostalim, i ovdje je privola jedno od takvih pravila ovlaštenja.

67. Iako priznaje sadržajnu sličnost korejskog zakona s Općom uredbom o zaštiti podataka s obzirom na načelo zakonitosti i postojanje općeg prava na obustavljanje (članak 37. PIPA-e) koji se može pozvati i ako se osobni podatci obrađuju na temelju privole, EDPB želi istaknuti nepostojanje općeg prava na povlačenje privole prema PIPA-i[23]. Uzimajući u obzir važnost privole kao pravne osnove u svim prethodno opisanim scenarijima te uzimajući u obzir ulogu prava pojedinca u pravnom sustavu zaštite podataka radi zaštite temeljnih prava i sloboda ispitanika, EDPB poziva Europsku komisiju da dodatno procijeni utjecaj nedostatka općenitog prava na povlačenje privole na temelju korejskog zakona te da pruži dodatna jamstva kako bi osigurala i da je u svakom trenutku zajamčena temeljna razina zaštite podataka kao što je ona predviđena Općom uredbom o zaštiti podataka, gdje je to potrebno, tako da se razjasni uloga prava na obustavljanje u ovom konkretnom kontekstu.

3.1.4. Načelo ograničenja svrhe

68. U Referentnom se dokumentu o primjerenosti Opće uredbe o zaštiti podataka, sukladno Općoj uredbi o zaštiti podataka, navodi da bi se osobni podatci trebali obrađivati za određenu svrhu i nakon toga upotrebljavati samo ako nije u suprotnosti od svrhe obrade.

69. Prema članku 3. stavku 1. i. 2. PIPA-e, voditelji obrade osobnih podataka trebaju odrediti i izričito navesti svrhu obrade te osigurati da je obrada u skladu s tom svrhom. Dok je načelo potvrđeno u drugim odredbama (npr. članci 15. stavak 1., 18. stavak 1. i 19. stavak 1. PIPA-e), obrada za „razumno povezane“ svrhe dozvoljena je u određenim okolnostima (vidjeti članak 17. stavak 4. PIPA-e)[24] te za upotrebu i pružanje osobnih podataka bez svrhe (vidjeti članke 18. i 19. PIPA-e)[25].

[23] Iako ispitanici mogu odbiti davanje privole o određenim okolnostima, vidjeti primjerice članak 18. stavak 3., 5. PIPA-e. S druge strane, čini se da pravo na povlačenje privole postoji samo u određenim slučajevima; u skladu s člankom 27. stavkom 1. PIPA-e, ispitanici imaju pravo na povlačenje privole ako ne žele da se njihovi osobni podatci prenose trećoj strani zbog prijenosa određenih ili svih poslovanja, udruživanja itd. voditelja obrade osobnih podataka; u skladu s člankom 39. stavkom 7. PIPA-e, korisnici mogu povući svoju privolu za prikupljanje, upotrebu i pružanje osobnih podataka u svakom trenutku od pružatelja usluga informiranja i komunikacije itd.; te prema članku 37. CIA-e, ispitanik osobnih kreditnih podataka može povući svoju privolu koja je prethodno pružena pružatelju/korisniku kreditnih podataka.

[24] Pri čemu se kompatibilnost svrhe mora ustanoviti unaprijed na temelju kriterija određenih u članku 14.-2. Provedbenog dekreta PIPA-e.

[25] Vidjeti i gore pod t. 66.

70. EDPB shvaća da se u slučaju prijenosa osobnih podataka iz EGP-a u Republiku Koreju na temelju odluke o primjerenosti, svrha prikupljanja voditelja obrade u EGP-u sastoji od svrhe za koju se podatci prenose, a koja je primjenjiva za obradu voditelja obrade osobnih podataka u Koreji koji ih primaju. Promjena svrhe koju izvršava voditelj obrade u Koreji bila bi dozvoljena samo kako je predviđeno u članku 18. stavku 2. točki 1. – 3. PIPA-e *„osim ako će to vjerojatno nepravedno kršiti interes ispitanika ili treće strane"*[26]. U tom kontekstu EDPB priznaje izjavu Europske unije u uvodnoj izjavi 55. nacrta odluke da, ako promjenu svrhe odobri zakon, takvi zakoni moraju poštivati temeljno pravo na privatnost i zaštitu podataka. Međutim, EDPB ističe da nisu pružene specifične informacije koje podržavaju ovu određenu izjavu, primjerice, nije se pozvalo na članak 37. (korejskog) ustava. Stoga EDPB poziva Europsku komisiju na davanje dodatnih pojašnjenja i jamstava u nacrtu odluke kako bi se osiguralo da se svakim zakonom koji odobrava promjenu svrhe obrade moraju poštovati temeljna prava i slobode ispitanika na privatnost i zaštitu podataka.

3.1.5. Kvaliteta podataka i načelo proporcionalnosti

71. Referentni dokument o primjerenosti Opće uredbe o zaštiti podataka navodi da bi podatci trebali bit točni i, ako je potrebno, ažurirani. Podatci bi trebali biti primjereni i relevantni te da nisu pretjerani u odnosu na svrhe u koje se obrađuju.

72. Prema PIPA-i, voditelji obrade osobnih podataka moraju osigurati da su osobni podatci točni, potpuni i ažurirani u mjeri potrebnoj u odnosu na svrhu u koju se obrađuju osobni podatci (članak 3. stavak 3. PIPA-e). Voditelji obrade osobnih podataka moraju prikupljati što manje osobnih podataka koliko je potrebno za postizanje zadane svrhe. U tom smislu nose teret dokazivanja (članak 16. stavak 1. PIPA-e).

73. EDPB na temelju ovoga dijeli procjenu Europske komisije s obzirom na načelnu istovjetnost razine zaštite prema PIPA-i u pogledu Opće uredbe o zaštiti podataka.

3.1.6. Načelo zadržavanja podataka

74. U skladu s referentnim dokumentom o primjerenosti Opće uredbe o zaštiti podataka, kao opće pravilo, podatci se ne bi trebali pohranjivati dulje nego što je potrebno za svrhe u koje se osobni podatci obrađuju. Prema članku 21. stavku 1. PIPA-e, ta načela postoje i u korejskom pravu. Prema PIPA-i, voditelji obrade osobnih podataka moraju uništiti osobne podatke bez odgode kad osobni podatci postanu nepotrebni nakon isteka razdoblja zadržavanja ili nakon postizanja namjeravane svrhe obrade, osim ako se ne primjenjuju zakonska razdoblja zadržavanja.

75. Međutim, EDPB je zabrinut činjenicom da članak 21. stavak 1. PIPA-e nije primjenjiv za pseudonimizirane osobne podatke. EDPB ističe činjenicu da, u skladu s Odjeljkom 4. iii. Obavijesti br. 2021-1, „kad voditelj obrade osobnih podataka obrađuje pseudonimizirane podatke u svrhe izrade statike, znanstvenog istraživanja, očuvanja javnih spisa itd. te ako pseudonimizirani podatci nisu *[sic]* uništeni kad je ispunjena određena svrha obrade u skladu s člankom 37. Ustava i člankom 3. (Načela zaštite osobnih podataka) Zakona, anonimizirat će podatke kako bi osigurao da više ne identificiraju određenog pojedinca, sami ili u kombinaciji s drugim podatcima, uzimajući razumno u obzir vrijeme, trošak, tehnologiju itd. u skladu s člankom 58. stavkom 2. PIPA-e". S obzirom na opetovanu važnost Obavijesti 2021-1 te radi pravne sigurnosti glede istovjetnosti razine zaštite osobnih podataka koji se prenose u Republiku Koreju na temelju odluke o primjerenosti, EDPB ponavlja svoj poziv Europskoj komisiji na davanje dodatnih informacija posebice o tome kako Obavijest br. 2021-1 postaje obvezujuća te na koji se način osiguravaju njezina provedivost i valjanost[27].

[26] Članak 18. stavak 2. PIPA-e.

[27] Vidjeti i prethodnu t. 51. u odjeljku 3.1.1.1. ovog mišljenja te t. 52. za opće zabrinutosti EDPB-a glede utjecaja pseudonimizacije prema korejskom zakonu.

3.1.7. Načelo sigurnosti i povjerljivosti

76. Kako je opisano u referentnom dokumentu o primjerenosti Opće uredbe o zaštiti podataka, načelo sigurnosti i povjerljivosti od subjekata obrade podataka zahtijeva jamstvo da se osobni podatci obrađuju na način koji osigurava njihovu sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade i od nenamjernog gubitka, uništenja ili oštećenja, upotrebom odgovarajućih tehničkih i organizacijskih mjera. Razina sigurnosti u obzir bi trebala uzeti najsuvremenije i povezane troškove.

77. Europska komisija prepoznala je slično načelo sigurnosti podataka u članku 3. stavku 4. PIPA-e koje je detaljnije navedeno u članku 29. PIPA-e. Osim toga, odredbe sigurnosti podataka primjenjuju se ako voditelj obrade osobnih podataka zaposli „vanjskog suradnika". Sigurnost obrade mora se zajamčiti tehničkim i upravljačkim zaštitnim mjerama koje ujedno moraju biti uključene u obvezujući sporazum o obradi podataka (članak 26. PIPA-e i članak 28. Provedbenog dekreta PIPA-e). Nadalje, specifične obveze prema PIPA-i primjenjuju se u slučaju povrede podataka, uključujući obveze obavještavanja pogođenih ispitanika i nadzorno tijela ako broj pogođenih ispitanika prelazi primjenjivi prag (članak 34. PIPA-e u vezi s člankom 39. Predsjedničkog dekreta PIPA-e), osim ako su pogođeni podatci pseudonimizirani osobni podatci obrađeni u svrhe statistike, znanstvenog istraživanja ili arhiviranja od javnog interesa (članak 28. stavak 7. PIPA-e). I ovdje[28] je EDPB zabrinut za opsežna izuzeća za pseudonimizirane podatke te ponavlja svoj poziv Europskoj komisiji za daljnju procjenu ovog aspekta kako bi se osiguralo da je razina zaštite u načelu istovjetna onoj pruženoj prema korejskom zakonu[29].

78. Bez obzira na to, EDPB je ukratko zadovoljan procjenom i zaključkom Europske komisije o načelnoj istovjetnosti korejskog zakona s obzirom na načelo sigurnosti i povjerljivost.

3.1.8. Načelo transparentnosti

79. Na temelju članka 5. stavka 1. točke (a) Opće uredbe o zaštiti podataka, transparentnost je temeljno načelo sustava EU-a za zaštitu podataka. Uvodna izjava 39. Opće uredbe o zaštiti podataka govori o ovom načelu navodeći da „*[bi] za pojedince trebalo biti transparentno kako se osobni podatci koji se odnose na njih prikupljaju, upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti osobni podatci obrađuju ili će se obrađivat*i. *(...) Fizičkim bi se osobama trebali pojasniti rizici, pravila, zaštitne mjere i prava povezana s obradom osobnih podataka te na koji način mogu ostvariti svoja prava kad je riječ o takvoj obradi*."

80. Referentni dokument o primjerenosti Opće uredbe o zaštiti podataka izričito navodi „transparentnost" kao jedno od načela sadržaja koje je potrebno uzeti u obzir pri procjeni načelne istovjetnosti razine zaštite koju pruža treća zemlja. Detaljnije, navodi da bi „*svaki pojedinac trebao biti obaviješten o svim glavnim elementima obrade njegovih/njenih osobnih podataka na jasan, jednostavno dostupan, sažet, transparentan i razumljiv način*. *Takve bi informacije trebale sadržavati svrhu obrade, identitet voditelja obrade podataka, prava koja su mu/joj pružena i druge informacije koje su potrebne za osiguranje pravednosti. Pod određenim uvjetima mogu postojati izuzeća od ovog prava za informacijama, kao što su, primjerice, radi zaštite kaznenih istraga, nacionalne sigurnosti, nezavisnosti pravosuđa i sudskih postupaka ili drugih važnih ciljeva od općeg javnog interesa kao što je slučaj s člankom 23. Opće uredbe o zaštiti podataka*."

81. Slično kao što je slučaj s Općom uredbom o zaštiti podataka, prema PIPA-i postoji opće načelo transparentnosti koje od voditelja obrade osobnih podataka traži javno objavljivanje svoje politike zaštite privatnosti i drugih stvari povezanih s obradom osobnih podataka (članak 3. stavak 5. PIPA-e.). Specifične obveze informiranja primjenjuju se ako voditelji obrade osobnih podataka traže dobivanje privole od ispitanika za prikupljanje i obradu osobnih podataka (članak 15. stavak 2. PIPA-e), za dijeljenje osobnih podataka s trećom stranom (članak 17. stavak 2. PIPA-e) te za nenamjensku obradu

[28] Kako je već navedeno u prethodnim t. 51-52 i odjeljku 3.1.1.1. ovog Mišljenja.
[29] Vidjeti i odjeljke 3.1.6. i 3.1.10. ovog Mišljenja.

podataka (članak 18. stavak 3. PIPA-e). Važno je napomenuti da se ove obveze informiranja primjenjuju i *mutatis mutandis* na vanjskog suradnika (članak 26. stavak 7. PIPA-e).

82. EDPB priznaje i pozdravlja dodatne zaštitne mjere u Odjeljku 3. točkama (i) i (ii) Obavijesti br. 2021-1[30] za pružanje informacija ispitanicima ako se njihovi podatci prenose od subjekta u EGP-u, uzimajući u obzir činjenicu da se, prema članku 20. stavku 1. PIPA-e, ako podatci nisu dobiveni od ispitanika, ispitanici obavještavaju samo na zahtjev, dok se opće pravo na informiranje prepoznaje samo u skladu s člankom 20. stavkom 2. PIPA-e ako određeni postupci obrade prelaze prag određen Provedbenim dekretom PIPA-e (članak 15. stavak 2.).

83. EDPB je općenito zadovoljan činjenicom da je razina zaštite prema korejskom pravu s obzirom na načelo transparentnosti u načelu istovjetna onoj predviđenoj Općom uredbom o zaštiti podataka.

3.1.9. Posebne kategorije osobnih podataka

84. Kako bi se priznalo da sustav zaštite treće zemlje pruža razinu zaštite osobnih podataka u načelu istovjetnu onoj iz Opće uredbe za zaštitu podataka, trebale bi postojati određene zaštitne mjere ako je riječ o posebnim kategorijama osobnih podataka unutar značenja članaka 9. i 10. Opće uredbe o zaštiti podataka.

85. Prema PIPA-i, određene odredbe vrijede za obradu takozvanih osjetljivih podataka koji uključuju osobne podatke koji otkrivaju ideologiju, vjerovanje, uvrštenje ili povlačenje iz sindikata ili političke stranke, politička mišljenja, zdravlje, seksualni život i druge osobne podatke koji će vjerojatno izrazito ugroziti privatnost svakog ispitanika te, pozivajući se na Provedbeni dekret PIPA-e, podatke o DNK-u dobivenih genetskim ispitivanjem, podatke koji uključuju zapise o kažnjavanju, osobne podatke koji su rezultat određene tehničke obrade podataka povezanih s fizičkim i fiziološkim karakteristikama ili obrascima ponašanja pojedinca u svrhu jedinstvene identifikacije tog pojedinca te osobne podatke koji otkrivaju rasno ili etničko podrijetlo.

86. Slično Općoj uredbi o zaštiti podataka, korejski zakon za zaštitu podataka zabranjuje obradu osjetljivih podataka osim ako se primjenjuju specifična izuzeća koja se sastoje od: (1) obavještavanja ispitanika i dobivanje određene privole te (2) zakonskih odredbi kojima se odobrava obradu (članak 23. stavak 2. PIPA-e).

87. EDPB se na temelju toga u načelu slaže sa zaključkom Europske komisije o bitnoj ekvivalentnosti korejskog zakona s obzirom na obradu posebnih kategorija osobnih podataka. Međutim, EDPB bi želio istaknuti da to nije navedeno u priručniku za PIPA-u ni u objašnjenjima PIPC-a za pojam „seksualni život" koji se tumači kao da obuhvaća i spolnu orijentaciju pojedinca, što nije uključeno u Obavijest br. 2021-1. EDPB stoga poziva Europsku komisiju na pružanje ovih informacija kako bi ih procijenili neovisno. Nadalje, EDPB poziva Europsku komisiju da posebice navede dokumente u kojima se mogu pronaći informacije na koje se ovo odnosi.

3.1.10. Prava na pristup, ispravak, brisanje i prigovor

88. U korejskom pravnom okviru prava ispitanika priznaju se u članku 3. stavku 5. PIPA-e prema kojem voditelj obrade osobnih podataka treba jamčiti prava ispitanika navedena u članku 4. PIPA-e i dodatno određena u člancima od 35. do 37., članku 39. i članku 39. stavku 2. PIPA-e te, „osobni kreditni podatci" (odnosno, „kreditni podatci su podatci koji su potrebni kako bi se odredila kreditna sposobnost stranaka za financijske ili komercijalne transakcije", vidjeti uvodnu izjavu 3. nacrta odluke) u članku 37., članku 38. i članku 38. stavku 3. CIA-e.

89. EDPB ističe da se pravo na pristup (i ispravak i brisanje koje može ostvariti „ispitanik koji je pristupio svojim osobnim podatcima u skladu s člankom 35." PIPA-e) može ograničiti ili odbiti „*ako je pristup*

[30] Prilog I. nacrta odluke.

zabranjen ili ograničen zakonima“, „*ako bi pristup mogao ugroziti život ili tijelo treće strane ili predstavljati neopravdanu povredu imovine i drugih interesa bilo koje druge osobe*“ te dodatno za javne ustanove, ako bi odobravanje pristupa „*moglo uzrokovati velike poteškoće*“ pri provedbi određenih funkcija, što je dodatno pojašnjeno u članku 35. stavku 4. PIPA-e[31]. Slične odredbe sadržane su i članku 37. PIPA-e, a odnose se na pravo na obustavu obrade osobnih podataka.

90. Članom 23. Opće uredbe o zaštiti podataka dozvoljava se da se pravom Unije ili države članice ograniče prava pojedinca kad takvo ograničenje poštuje bit temeljnih prava i sloboda te kad je potrebna i razmjerna mjera u demokratskom društvu te kojom se predviđaju takve mjere radi čuvanja, među ostalim, zaštite ispitanika ili prava i sloboda drugih te „*praćenje, provjeru ili regulatornu funkciju povezanu, čak i povremeno, s izvršavanjem javnih ovlasti u slučajevima iz točki (a) do (e) i točke (g) istog članka*“.

91. EDPB bi na temelju ovoga pozdravio opća jamstva u nacrtu odluke o potrebi za svakim zakonom ili statutom koji ograničava prava ispitanika kako bi se ispunili zahtjevi korejskog ustava da se temeljno pravo može ograničiti samo kad je to potrebno radi nacionalne sigurnosti ili održavanja zakona i reda radi javnog dobra te da ta ograničenja ne smiju utjecati na bit predmetne slobode ili prava (članak 37. stavak 2. korejskog ustava).

92. Nadalje, s obzirom na iznimku povezanu s „*neopravdanom povredom imovine ili drugih interesa svake druge osobe*“, EDPB priznaje da to „*znači da bi trebalo doći do ravnoteže između prava i sloboda pojedinca zaštićenih ustavom s jedne strane i drugih osoba s druge strane*“[32], međutim, pozvao bi Europsku komisiju na potpuno praćenje primjene ovog izuzeća i relevantne sudske prakse kako bi se osiguralo da je zajamčena istovjetna razina zaštite prava ispitanika i u praksi u korejskom pravnom okviru.

93. EDPB bi jednako tako pozdravio pozorno praćenje primjene izuzeća za javna tijela, posebice s obzirom na slučajeve u kojima bi se smatralo da dodjeljivanje pristupa uzrokuje „*velike poteškoće*“ u izvršavanju svojih dužnosti uzimajući u obzir da se ovaj izraz čini širim od onoga upotrijebljenog u drugim odredbama PIPA-e, npr. u članku 18. stavku 2. točki 5.[33] te da bi se trebao tumačiti restriktivno kako bi se izbjeglo neprimjereno ograničavanje prava ispitanika.

94. Osim toga, EDPB pokazuje zabrinutost u vezi toga jesu li izuzeća, prema kojima se ne primjenjuju odredbe o transparentnosti na zahtjev (članak 20. PIPA-e) i pravima pojedinca (članci 35. do 37. PIPA-e) – kao i slična pitanja koja se odnose na zahtjeve za pružatelje usluga informiranja i komunikacije (članak 39. stavak 2., članak 39. stavci od 6. do 8. PIPA-e) i ona sadržana u CIA-i (vidjeti izuzeća predviđena člankom 40. stavkom 3. CIA-e) – uzimajući u obzir pseudonimizirane podatke, kad se to obrađuje u svrhe statistike, znanstvenog istraživanja ili arhiviranja u javnom interesu (članak 28. stavak 7. PIPA-e), sukladna zaštitnim mjerama pruženima u europskom pravnom okviru.

95. Čini se da ove odredbe uvode opće odstupanje za takvu vrstu obrade, dok Opća uredba o zaštiti podataka predviđa da, ako se osobni podatci (uključujući pseudonimizirane osobne podatke) obrađuju u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, pravo Unije ili države članice može predvidjeti odstupanje od prava ispitanika ali „*u mjeri u kojoj je vjerojatno da bi se takvim pravima moglo onemogućiti ili ozbiljno ugroziti postizanje tih posebnih svrha te su takva odstupanja neophodna za postizanje tih svrha*“, pseudonimizacija je samo jedno od tehničkih i organizacijskih mjera koje se

[31] Jednaki uvjeti i iznimke od prava pristupa i ispravka predviđeni PIPA-om primjenjuju se i s obzirom na pravo pristupa i ispravka predviđeno za osobne kreditne podatke koje ima CIA (bilješka 135. nacrta odluke).
[32] Uvodna izjava 76. nacrta odluke.
[33] U odnosu na izuzeća na ograničenje upotrebe bez svrhe i davanje osobnih podataka, članak 18. stavak 2. točka 5. PIPA-e odnosi se na situaciju u kojoj je za javne ustanove „*nemoguće*“ izvršavati obveze.

moraju primijeniti kako bi se osiguralo poštovanje načela smanjenja količine podataka (članak 89. stavak 1. Opće uredbe o zaštiti podataka).

96. Europska unija smatra da je odstupanje koje je predviđeno člankom 28. stavkom 7. PIPA-e trebalo opravdati i u smislu članka 28. stavka 5. PIPA-e prema kojemu je voditelju obrade osobnih podataka izričito zabranjena obrada pseudonimiziranih podataka u svrhu identifikacije određenog pojedinca te se odnosi na pristup članka 11. stavka 2. Opće uredbe o zaštiti podataka (u vezi s uvodnom izjavom 57. Opće uredbe o zaštiti podataka) za obradu koja ne zahtjeva identifikaciju[34].

97. Zaista, u skladu s člankom 11. Opće uredbe o zaštiti podataka, voditelj obrade nije obvezan „*zadržavati, stjecati ili obrađivati dodatne informacije radi identificiranja ispitanika*“ samo u svrhu poštovanja Opće uredbe o zaštiti podataka ako, za namijenjenu svrhu, može obrađivati osobne podatke koji ne zahtijevaju ili više ne zahtijevaju identifikaciju ispitanika. U takvim slučajevima, kad voditelj obrade može pokazati da nije u mogućnosti identificirati ispitanika, ne primjenjuju se prava ispitanika. Kako je potvrdila Europska komisija[35], Opća uredba o zaštiti podataka stoga u takvim slučajevima zahtjeva „praktičnu“ nemogućnost za voditelja obrade te, u skladu s načelom smanjivanja količine podataka, prepoznaje da se ne moraju obrađivati dodatni podatci „zbog“ Opće uredbe o zaštiti podataka.

98. Međutim, EDPB smatra da je ova situacija različita od one u kojoj je voditelj obrade praktički u mogućnosti identificirati ispitanika, ali nije mu dozvoljeno to učiniti prema zakonskoj odredbi kao što je ona u članku 28. stavku 5. PIPA-e. Glede toga, EDPB pozdravlja objašnjenja koja je dao PIPC u Obavijesti br. 2021-1[36] u kojoj je potvrdio da se Odjeljak 3. PIPA-e (uključujući članak 28. stavak 7.) i izuzeće članka 40. stavka 3. CIA-e primjenjuje samo kad se pseudonimizirani podatci obrađuju za znanstvena istraživanja, statistiku ili arhiviranje od javnog interesa. Međutim, uz već navedenu zabrinutost zbog djelotvornog obvezujućeg učinka Obavijesti br. 2021-1[37], EDPB još uvijek razmatra mogu li se odstupanja predviđena člankom 28. stavkom 7. PIPA-e i članak 40. stavak 3. CIA-e smatrati potrebnim i proporcionalnim u demokratskom društvu jer ograničavaju prava ispitanika u svim slučajevima u kojima se pseudonimizirani podatci obrađuju u takve svrhe. Odnosno, čak i ako je voditelj obrade osobnih podataka praktično u mogućnosti identificirati ispitanika te takva prava vjerojatno neće onemogućiti ili ozbiljno ugroziti postignuća određenih svrha.

99. EDPB posebice izražava zabrinutosti da ta odstupanja ne bi bila opravdana te da bi se trebala dodatno pregledati, posebice ako ih primjenjuje voditelj obrade osobnih podataka koji pseudonimizira podatke „*u svrhe statistike, znanstvenog istraživanja ili svrhe arhiviranja od javnog interesa itd.*“ u skladu s člankom 28. stavkom 2. PIPA-e „*bez privole ispitanik*a“ (i bez pružanja podataka predviđenih člankom 20. PIPA-e)[38], sve dok taj voditelj obrade zadržava podatke koji omogućuju ponovnu identifikaciju. Prema Općoj uredbi o zaštiti podataka pojedinci bi trebali biti u mogućnosti ostvariti svoja prava povezana sa svim podatcima koji bi ih mogli identificirati ili izdvojiti, čak i kad se podatci smatraju „pseudonimiziranim“, osim ako se ne primjenjuje već spomenuti članak 11. Opće uredbe o

[34] Ističe se da jednako mišljenje ne bi bilo primjenjivo kao takvo na izuzeće predviđeno člankom 40. stavkom 3. CIA-e za obradu pseudonimiziranih kreditnih podataka jer članak 40. stavak 2. točka 6. predviđa da: „*Tvrtka koja ima kreditne informacije itd. neće obrađivati pseudonimizirane podatke na način na koji bi se određeni pojedinac mogao identificirati u svaku profitabilnu ili nepravednu svrhu*“ te bi stoga mogla odobriti ponovnu identifikaciju u pravednu svrhu kao što je ispunjavanje zahtjeva ispitanika.

[35] Vidjeti uvodnu izjavu 82. nacrta odluke.

[36] Odjeljak 4. Priloga I. nacrta odluke.

[37] Vidjeti prethodni odjeljak 3.1.1.1.

[38] Vidjeti članak 28. stavak 7. PIPA-e, kako je objašnjeno u Obavijesti br. 2021-1, prema kojoj se određene zaštitne mjere sadržane u PIPA-i, odnosno „*članci 20., 21., 27., članak 34. stavak 1., članci od 35. do 37., 39. stavci 3. i 4., članak 39. stavci od 6. do 8.*“ ne odnose na pseudonimizirane podatke koji se obrađuju u svrhu prikupljanja statistike, znanstvenih istraživanja, održavanja javnih spisa itd.

zaštiti podataka. Prema tome, EDPB ističe da samo kad se ti podatci pružaju trećoj strani za jednake svrhe statistike, znanstvenog istraživanja i arhiviranja, ne smiju se uključiti podatci koji bi se mogli upotrijebiti za identifikaciju određenog pojedinca te bi stoga samo voditelj obrade osobnih podataka kojemu su pruženi pseudonimizirani podatci, u skladu s člankom 28.-2. stavkom 2. PIPA-e vjerojatno „praktički" ne bi bio u mogućnosti identificirati ispitanika bez dodatnih podataka.

100. Ukratko, uzimajući u obzir da, budući da Europska komisija priznaje „*umjesto oslanjanja na pseudonimizaciju kao moguću zaštitnu mjeru, PIPA je nameće kao preduvjet za provođenje određenih aktivnosti obrade u svrhu statistike, znanstvenog istraživanja i arhiviranja u javnom interesu (kao što je mogućnost obrade podataka bez privole ili kombiniranja različitih skupova podataka)*"[39], ali za takve slučajeve predviđa važna ograničenja prava ispitanika, EDPB poziva Europsku komisiju na daljnju procjenu odstupanja sadržanih u članku 28. stavku 7. PIPA-e i članku 40. stavku 3. CIA-e te na pomno praćenje primjene i relevantne sudske prakse[40] kako bi se osiguralo da se prava ispitanika neopravdano ne ograničavaju kad se osobni podatci preneseni pod odlukom o primjerenosti obrađuju u ove svrhe uzimajući u obzir da, u mnogim slučajevima, ova prava pomažu voditelju obrade osigurati kvalitetu obrađenih podataka.

3.1.11. Ograničenja daljnjih prijenosa

101. Referentni dokument o primjerenosti Opće uredbe o zaštiti podataka objašnjava da se razina zaštita fizičke osobe čiji se osobni podatci prenose u sklopu odluke o primjerenosti ne smije narušavati daljnjim prijenosom te bi stoga svaki daljnji prijenos „*trebao biti dozvoljen samo ako daljnji primatelj (odnosno, primatelj daljnjeg prijenosa) isto podliježe pravilima (uključujući ugovorna pravila) pružajući primjerenu razinu zaštite i slijedeći relevantne upute ako se obrađuju podatci u ime voditelja obrad*e".

102. Kad je riječ o daljnjem prijenosu vanjskim suradnicima (odnosno „izvršiteljima obrade") što je uspostavljeno u ostalim trećim zemljama, EDPB ističe da u korejskom pravnom okviru ne postoje određena pravila koja obuhvaćaju takve slučajeve te da, prema Europskoj komisiji[41], korejski voditelj obrade osobnih podataka mora osigurati sukladnost s odredbom PIPA-e o eksternalizaciji (članak 26. PIPA-e) legalno obvezujućim instrumentom i da će biti odgovoran za osobne podatke koji su eksternalizirani (članak 26. PIPA-e).

103. S obzirom na daljnje prijenose trećim stranama (odnosno, drugim voditeljima obrade osobnih podataka), u skladu s člankom 17. stavkom 3. PIPA-e, korejski voditelj obrade osobnih podataka mora obavijestiti ispitanika o tome i dobiti njegovu privolu za prekomorske prijenose te „*neće sklopiti ugovor za prekogranični prijenos osobnih podataka i kršiti odredbe PIPA-e*". EDPB ističe da ova posljednja odredba jamči da, prema Europskoj komisiji[42], ugovori za prekogranične prijenose ne smiju sadržavati obveze koje su proturječne zahtjevima propisanima PIPA-om o voditelju obrade osobnih podataka i stoga se mogu smatrati zaštitnom mjerom, međutim, ne nameću nikakvu obvezu uspostavljanja zaštitnih mjera kako bi se zajamčilo da će primatelj osigurati jednaku razine zaštite koju pruža PIPA. EDPB stoga priznaje da će se informirana privola ispitanika općenito shvatiti kao temelj prijenosa podataka od voditelja obrade osobnih podataka u Koreji primatelju u trećoj zemlji.

104. Prema tome, dodatna objašnjenja koja je pružio PIPC u Obavijesti br. 2021-1 o obvezi obavještavanja pojedinca o trećoj zemlji kojoj će njihovi podatci biti pruženi[43] pozdravljaju se jer bi, kako naglašava

[39] Uvodna izjava 42. nacrta odluke.
[40] Vidjeti, primjerice, ustavne izazove organizacije Opet Net (informacije na https://opennet.or.kr/19909 dostupne su samo na korejskom).
[41] Uvodna izjava 87. nacrta odluke.
[42] Uvodna izjava 88. nacrta odluke.
[43] Ibid.

Europska komisija[44], pomogli ispitanicima u EGP-u u donošenju potpuno utemeljene odluke o tome trebaju li dati privolu za prekomorsko pružanje.

105. Međutim, što je napomenuto u Mišljenju 28/2018 o Nacrtu provedbene odluke Europske komisije o odgovarajućoj zaštiti osobnih podataka u Japanu, potrebno je naglasiti da, prema Općoj uredbi o zaštiti podataka, ispitanici moraju biti izričito obaviješteni o mogućim rizicima takvih prijenosa koji nastaju zbog nepostojanja primjerene zaštite u trećoj zemlji i nepostojanja odgovarajućih zaštitnih mjera prije privole. Takva bi obavijest trebala sadržavati, primjerice, informacije da možda ne postoje nadzorno tijelo i/ili načela obrade podataka i/ili prava ispitanika u trećoj zemlji[45]. EDPB smatra da je pružanje tih informacija ključno kako bi ispitanik mogao dati informiranu privolu te da je u potpunosti upoznat sa specifičnim činjenicama prijenosa[46]. Stoga EDPB izražava zabrinutost u pogledu nalaza Europske komisije u nacrtu odluke o primjerenosti glede specifičnih vrsta prijenosa. Ispitanici obično nisu upoznati s okvirom zaštite podataka u trećim zemljama. Stoga se ne može zaključiti da bi ispitanik mogao procijeniti rizik prijenosa poznavajući samo specifičnu zemlju odredišta. Naprotiv, trebaju postojati jasne informacije o specifičnim rizicima takvog prijenosa osobnih podataka u zemlju izvan državnog područja Republike Koreje prije privole ispitanika.

106. Stoga EDPB poziva Europsku komisiju da osigura da će informacije koje će biti pružene ispitaniku „*o okolnostima prijenosa*“ sadržavati informacije o mogućim rizicima prijenosa koji nastaju zbog nedostatka odgovarajuće zaštite u trećoj zemlji i odgovarajućih zaštitnih mjera. To je važno za EDPB kako bi procijenio jesu li zahtjevi za privolu u načelu istovjetni onima iz Opće uredbe za zaštitu podataka.

107. Nadalje, s obzirom na to da bi privola trebala biti dana dobrovoljno, informirano, specifično i jasno, EDPB bi pozdravio jamstva u odluci o primjerenosti da korejski voditelji obrade osobnih podataka neće prenositi osobne podatke trećoj strani u treću zemlju u situacijama u kojima se, prema Općoj uredbi o zaštiti podataka, nije mogla pružiti valjana privola, npr. zbog neravnoteže moći.

108. Povezano sa slučajevima u kojima voditelj obrade osobnih podataka može prekomorski pružiti osobne podatke trećoj strani bez privole ispitanika, odnosno, (1) ako su osobni podatci pruženi unutar opsega koji je razumno povezan s prvotnom svrhom prikupljanja u skladu s člankom 17. stavkom 4. PIPA-e; i (2) ako se osobni podatci mogu pružiti trećoj strani u iznimnim slučajevima spomenutima u članku 18. stavku 2. PIPA-e, EDPB ističe objašnjenje koje je dalo PIPC u odjeljku 2. Obavijesti br. 2021-1 (te pozdravlja predviđenu obvezu izrečenu voditelju obrade u Koreji i prekomorskom primatelju kako bi se pravno obvezujućim instrumentom (kao što je ugovor) osigurala razina zaštite ekvivalentna onoj u PIPA-i, među ostalim za prava ispitanika).

3.1.12. Izravni marketing

109. Prema članku 21. stavcima 2. i 3. Opće uredbe o zaštiti podataka i referentnom dokumentu o primjerenosti Opće uredbe o zaštiti podataka, ispitanik uvijek mora biti u mogućnosti prigovora bez naplate obrade podataka u svrhe izrade profila i izravnog marketinga.

110. S obzirom na pravo na obustavu predviđeno člankom 37. PIPA-e, EDPB priznaje da Europska komisija smatra da se ovo pravo primjenjuje i ako se podatci upotrebljavaju u svrhe izravnog marketinga[47]. Međutim, EDPB bi pozdravio dodatne informacije i objašnjenja u nacrtu odluke o ovoj procjeni te posebice o praktičnoj primjeni prava na obustavu u kontekstu izravnog marketinga (npr. pozivanje na relevantnu sudsku praksu itd.). U tom smislu EDPB bi ujedno htio naglasiti da je pravo na traženje od

[44] Ibid.
[45] Smjernice EDPB-a 2/2018 o odstupanjima od članka 49. prema Uredbi 2016/679, 25. svibnja 2018., str. 8.
[46] Smjernice EDPB-a 2/2018 o odstupanjima od članka 49. prema Uredbi 2016/679, 25. svibnja 2018., str. 7.
[47] Uvodna izjava 79. nacrta odluke.

pružatelja/korisnika kreditnih podataka da prestane kontaktirati s njima u svrhu predstavljanja ili poticanja prodaje roba ili usluga izričito određeno u CIA-u (članak 37. stavak 2.).

111. Nadalje, kako priznaje Europska komisija[48] u korejskom pravnom okviru takva obrada općenito zahtijeva specifičnu (dodatnu) privolu ispitanika (vidjeti članak 15. stavak 1. točka 1., članak 17. stavak 2. točka 1. PIPA-e).

112. S obzirom na to da se ne može isključiti da će se podatci preneseni iz EGP-a u Koreji obrađivati u takve svrhe, EDPB bi pozdravio i objašnjenja u odluci o primjerenosti o postojanju prava ispitanika na povlačenje privole[49] i prava na brisanje svojih osobnih podataka i prestanak obrade ako se obrada temelji na privoli (kao što je slučaj obrade koja se provodi u marketinške svrhe), a ispitanik ju je povukao.

3.1.13. Automatizirano donošenje odluka i izrada profila

113. Kao što je Europska komisija priznala u nacrtu odluke[50], PIPA i njezin Provedbeni dekret ne sadržavaju opće odredbe za pitanje odluka koje utječu na ispitanika i koje se temelje isključivo na automatiziranoj obradi osobnih podataka. No, korejski pravni sustav predviđa takvo pravo u CIA-i koja sadržava pravila o automatiziranim odlukama (članak 36. stavak 2.) čak i kad se čini da je njihova primjena izvan područja nadzora PIPC-a (te, kao takva, izvan područja primjene ovog nacrta odluke, vidjeti prethodni odjeljak 2.3.2. o području primjene nacrta odluke).

114. Kao što je već spomenula Radna skupina[51] za članak 29., prema njezinu Mišljenju 1/2016 o sustavu zaštite privatnosti i prema EDPB-u u svojem prethodnom mišljenju o odluci o primjerenosti koja se odnosi na Japan[52], zbog sve veće važnosti automatiziranog donošenja odluke, izrade profila i umjetne inteligencije predlaže se sigurniji pristup. Suprotno argumentima Europske komisije[53] prema kojima nepostojanje određenih pravila o automatiziranom donošenju odluka u PIPA-i vjerojatno neće utjecati na razinu zaštite za osobne podatke koji su prikupljeni u Uniji (s obzirom na to da bi svaku odluku na temelju automatizirane obrade obično donio voditelj obrade u Uniji koji ima izravan odnos s dotičnim ispitanikom), EDPB smatra da se ne može isključiti da bi automatizirano donošenje odluka mogao upotrebljavati voditelj obrade osobnih podataka u Koreji u slučaju prijenosa podataka prema odluci o primjerenosti (primjerice, u kontekstu zapošljavanja, za procjenu učinkovitosti na poslu, pouzdanosti, ponašanja itd.).

115. Razvoj novih tehnologija omogućuje tvrtkama jednostavnije provođenje ili razmatranje provođenja sustava za automatizirano donošenje odluka što bi moglo dovesti do oslabljivanja položaja pojedinaca. Ako odluke koje su donesene isključivo putem takvih automatiziranih sustava utječu na pravno stanje pojedinaca ili značajno utječu na njih (primjerice, uvrštavanjem pojedinaca na crnu listu i time oduzimanjem njihovih prava), ključno je predvidjeti dostatne zaštitne mjere, uključujući pravo na informiranost o određenim razlozima na kojima se temelji odluka i upotrijebljenoj logici, kako bi se

[48] Ibid.

[49] Vidjeti i prethodno pod t. 67.: Mogućnost opoziva privole jasno je predviđena u članku 37. stavku 1. CIA-e, no to se pravo spominje samo dvaput u PIPA-i za specifične okolnosti u člancima 27. stavku 1., točki (2.) i članku 39. stavku 7.

[50] Vidjeti uvodnu izjavu 81. nacrta odluke.

[51] Ova je Radna skupina uspostavljena sukladno članku 29. Direktive 95/46/EZ. Bila je neovisno savjetodavno tijelo Europske unije za područje zaštite osobnih podataka i privatnosti. Njezini se zadatci opisuju u članku 30. Direktive 95/46/EZ i članku 15. Direktive 2002/58/EZ. WP29 je u međuvremenu postao EDPB.

[52] Mišljenje 28/2018 o Nacrtu provedbene odluke Europske komisije o primjerenosti zaštite osobnih podataka u Japanu, doneseno 5. prosinca 2018.

[53] Uvodna izjava 81. nacrta odluke.

ispravile netočne ili nepotpune informacije te kako bi se osporila odluka ako je donesena na netočnoj činjeničnoj osnovi[54].

116. U tom je kontekstu EDPB zabrinut zbog nedostatka pravnih odredbi o automatiziranom donošenju odluka u PIPA-i te stoga poziva Europsku komisiju na rješavanje tog pitanja i nastavak praćenja razvoja korejskog pravnog okvira.

3.1.14. Odgovornost

117. Korejski pravni okvir sadržava različita pravila čiji je cilj osiguranje da voditelji obrade osobnih podataka primjenjuju odgovarajuće tehničke i organizatorske mjere kako bi stvarno bili usklađeni sa svojim obvezama zaštite podataka te kako bi mogli dokazati takvu usklađenost, među ostalim, nadležnom nadzornom tijelu. EDPB posebice pozdravlja postojanje pravila koja predviđaju primjenu internog plana upravljanja (članak 29. PIPA-e), obvezu provedbe takozvane procjene učinka na privatnost („**PIA**“) za slučajeve ako obrada predstavlja veći rizik od mogućih kršenja privatnosti (članak 33. stavak 1. PIPA-e i članak 35. Provedbenog dekreta PIPA-e), pravila o obuci i nadzoru osoblja (članak 28. PIPA-e) te obveze imenovanja službenika za zaštitu privatnosti (članak 31. PIPA-e povezan s člankom 32. Provedbenog dekreta PIPA-e).

118. EDPB dijeli mišljenje Europske unije o načelno istovjetnoj zaštiti koju jamči, čak i ako se čini da pravila relativno odstupaju od onih predviđenih Općom uredbom o zaštiti podataka, npr. nema odredbe koja navodi nužnost da službenik za zaštitu privatnosti treba biti neovisan, međutim, jasno je rečeno da on/ona mora podnositi izvješća upravi voditelju obrade osobnih podataka (članak 31. stavak 4. PIPA-e) i da on/ona ne smije neopravdano biti u nepovoljnom položaju kao posljedica provođenja ovih funkcija (članak 31. stavak 5. PIPA-e) te bi Europskoj komisiji mogao predložiti praćenje, pri pregledu odluke o primjerenosti, stvarne provedbe ovih odredbi kako bi se procijenila njihova učinkovita primjena.

3.2. Postupovni i provedbeni mehanizmi

119. Na temelju kriterija utvrđenih u referentnom dokumentu o primjerenosti Opće uredbe o zaštiti podataka, EDPB je analizirao sljedeće aspekte korejskog okvira za zaštitu podataka obuhvaćene nacrtom odluke: postojanje i učinkovito djelovanje neovisnog nadzornog tijela, postojanje sustava koji osigurava dobru razinu usklađenosti i sustava za pristup odgovarajućim mehanizmima pravne zaštite koji osiguravaju pojedincima u EGP-u sredstva za ostvarivanje njihovih prava i traženje pravne zaštite bez otežavajućih prepreka pristupu upravnoj i sudskoj zaštiti.

120. Sukladno Poglavlju VI. Opće uredbe o zaštiti podataka i Poglavlju 3. referentnog dokumenta o primjerenosti Opće uredbe o zaštiti podataka, mora postojati jedno ili više neovisnih nadzornih tijela čiji je zadatak praćenje, osiguravanje i primjena usklađenosti s odredbama zaštite podataka i privatnosti u trećoj zemlji kako bi se zajamčila istovjetna razina zaštite u EGP-u.

121. U tom kontekstu nadzorno tijelo treće zemlje mora djelovati potpuno neovisno i objektivno tijekom provedbe svojih zadataka i izvršavanju svojih ovlasti te pri tome ne bi trebalo tražiti ni prihvaćati upute. Osim toga, nadzorno tijelo trebalo bi imati sve nužne i raspoložive ovlasti i misije kako bi osiguralo usklađenost s pravima zaštite podataka i promoviralo osviještenost o tome. Trebalo bi se razmisliti i o osoblju i proračunu nadzornog tijela. Nadzorno tijelo mora isto tako biti u mogućnosti započinjati postupke na vlastitu inicijativu.

[54] WP 254, str. 7.

3.2.1. Nadležno neovisno nadzorno tijelo

122. U Republici Koreji neovisno tijelo zaduženo za praćenje i provedbu PIPA-e je PIPC. PIPC se sastoji od jednog predsjednika, potpredsjednika i sedam povjerenika. Predsjednika i potpredsjednika imenuje predsjednik države na preporuke predsjednika vlade. Dva se povjerenika imenuju na preporuku predsjednika, dva na preporuku predstavnikâ političke stranke kojoj pripada predsjednik države, a preostala tri člana na preporuku predstavnikâ drugih političkih stanaka (članak 7. stavak 2. točka 2. PIPA-e). PIPC-u pomaže tajništvo (članak 7. stavak 13.) i može uspostaviti potpovjerenstva (koje sa sastoji od tri povjerenika) koji se bave manjim kršenjima i pitanjima koja se ponavljaju (članak 7. stavak 12. PIPA-e).

123. EDPB u tom smislu priznaje da je, bez obzira na nedavnu reorganizaciju koja je uvelike izmijenila svoj status i ovlasti, PIPC uložio znatne napore u stvaranje potrebne infrastrukture kako bi se omogućilo uvođenje PIPA-e i najnovijih izmjena. Među tim naporima potrebno je navesti uspostavu pravila PIPC-a, razradu smjernica kako bi razjasnile tumačenje PIPA-e te uspostavu telefonske službe za pomoć kako bi davala savjete poslovnim subjektima i pojedincima o odredbama zaštite podataka kao i usluge posredovanja koja se bavi žalbama. Zadatci PIPC-a posebice uključuju savjetovanje o zakonima i propisima o zaštiti podataka, razvoju politika i smjernica za zaštitu podataka, istraživanju povreda prava pojedinaca, rješavanju žalbi, posredovanju u sporovima, provedbi usklađenosti s PIPA-om, osiguranju obuke i promidžbe u području zaštite podataka te razmjeni i suradnji s tijelima za zaštitu podataka trećih zemalja[55].

124. Imenovanje i sastav PIPC-a navedeni su u članku 7. stavku 2. PIPA-e. Iako je PIPC u nadležnosti predsjednika vlade (i predsjednika i potpredsjednika koje je imenovao predsjednik države na preporuku predsjednika vlade), pravni okvir nalaže da povjerenici svoje obveze provode neovisno u skladu s pravom i svojom savjesti. EDPB priznaje institucijske i postupovne zaštitne mjere sadržane u PIPA-i, u članku 7. stavcima od 4. do 7. Ipak, EDPB bi pozvao Europsku komisiju da prati svaku promjenu koja bi mogla utjecati na neovisnost članova nadzornog tijela Južne Koreje.

125. Štoviše, nacrt odluke još ne obuhvaća analizu proračuna PIPC-a, uključujući izvore financiranja i transparentnost proračuna. EDPB smatra da se ovaj element, koji se spominje i u članku 56. stavku 1. Opće uredbe o zaštiti podataka i u proceduralnim i provedbenim mehanizmima i načelima zaštite podataka koji se uzimaju u obzir prema referentnom dokumentu o primjerenosti Opće uredbe o zaštiti podataka kad se procjenjuje sustav zemlje ili međunarodne organizacije, mora temeljitije uzeti u obzir jer je pokazatelj gospodarskih i ljudskih potencijala raspoloživih nadzornom tijelu za neovisno provođenje svoji zakonskih obveza i zadataka zaštite podataka te bi stoga Europskoj komisiji preporučio njegovo detaljno razmatranje u nacrtu odluke.

3.2.2. Postojanje sustava za zaštitu podataka koji jamči dobru razinu usklađenosti

126. U području izvršenja, EDPB potvrđuje raspon ovlaštenja za izvršenje i sankcije PIPC-a kako je propisano u PIP-a i CIA-i te ističe objašnjenje sadržano u Obavijesti br. 2021-1 prema kojoj će uvjeti navedeni u člancima 64. stavku 1. PIPA-e i članku 45. stavku 4. CIA-e[56] biti primjenjivi kad god se budu kršila načela, prava i obveze, među ostalim u zakonu za zaštitu osobnih podataka. Međutim, preporučuje Europskoj komisiji pomno praćenje primjenu u praksi ovlaštenja PIPC-a za nalaganje kršitelju za podnošenje mjere koju smatra primjerenom među onima navedenima u članku 64. stavku 1. ili članku 45. stavku 4. CIA-e.

127. Nadalje, povezano s korektivnim mjerama navedenima u članku 64. stavku 1. PIPA-e, u slučaju nepoštivanja korektivnih mjera, PIPC-a ima ovlasti propisati novčanu kaznu u najvećem iznosu od 50 milijuna korejskih vona (članak 75. stavak 2. točka 13. PIPA-e). Taj je iznos jednak 36.564 EUR. EDPB

[55] Zadatci i ovlasti PIPC-a uglavnom su sadržani u člancima 7. stavku 8. i 9. te u člancima od 61. do 66. PIPA-e.
[56] Odnosno, „*kršenje zakona vjerojatno će povrijediti prava i slobode pojedinca s obzirom na osobne podatke, a nemogućnost poduzimanja radnje vjerojatno će uzrokovati štetu koju je teško ispraviti*“.

smatra i izražava zabrinutost da je takav ograničeni opseg novčanih sankcija možda neće imati posebno snažan preventivni učinak na kršitelje kakav je određen zakonom kako bi se osigurala provedba pravila zaštite podataka jer se odvraćanje ne čini primjereno i dostatno, posebice u slučaju velikih organizacija ili poduzeća sa znatnim financijskim resursima.

128. Uzimajući u obzir mogućnost da PIPC može zatražiti da predsjedavajući središnje administrativne agencije istraži voditelja obrade osobnih podataka ili zajedno pokrene istragu o kršenju PIPA-e te čak odredi korektivne mjere za voditelje obrade osobnih podataka prema njihovoj nadležnosti (članak 63. stavak 4.-5. PIPA-e), EDPB ističe da, iako su određene informacije dane u uvodnoj izjavi 122. nacrta odluke, općenito, narav tih drugih agencija i njihovih pravnih veza s PIPC-om ostaje nejasna. Dodatno, članak 68. stavak 1. PIPA-e odnosi se na mnoge subjekte koji bi bili u mogućnosti prenijeti ovlasti PIPC-a. Čak i ako se čini da je ova odredba primijenjena samo u odnosu na Korejsku agenciju za internet i sigurnost[57], EDPB bi pozdravio objašnjenja za prirodu mogućih interakcija između tih subjekata i pomnog praćenja primjene ove odredbe u budućnosti kako bi se osigurala neovisnost subjekata zaduženih za primjenu pravila za zaštitu podataka.

129. Kad je riječ o sankcijama, čini se da korejski sustav kombinira različite vrste sankcija, od korektivnih mjera i upravnih novčanih kazni do kaznenih sankcija koje će vjerojatno imati snažan preventivni učinak, a korejske su vlasti predstavile nekoliko primjena novčanih kazni koje je nedavno odredio PIPC, među ostalim, jedna u vrijednosti od 6,7 milijardi korejskih vona određenih u prosincu 2020. tvrtki za kršenje različitih odredbi PIPA-e te druga novčana kazna u iznosu od 103,3 milijuna korejskih vona 28. travnja 2021. izdana tvrtki koja se bavi umjetnom inteligencijom za kršenje pravila zakonitosti obrade, posebice privole te obrade pseudonimiziranih podataka.

130. Iako bi prethodno navedeni iznosi mogli imati preventivan učinak, EDPB bi pozdravio dodatne informacije o metodama koje je upotrijebio PIPC za izračun razine upravnih novčanih kazni, primjerice, za novčane kazne određene za nepoštivanje korektivne mjere izdane u skladu s člankom 64. stavkom 1. PIPA-e (vidjeti članak 75. stavak 2. točka 13. PIPA-e). To je posebice relevantno za kaznene sankcije i primjenu (korejskog) Kaznenog zakona.

3.2.3. Sustav za zaštitu podataka mora pružiti podršku i pomoć ispitanicima da ostvare svoja prava i odgovarajuće mehanizme pravne zaštite

131. Kad je riječ o pravnoj zaštiti, čini se da korejski sustav nudi različite načine jamstva za primjerenu zaštitu i, posebice, provedbe prava pojedinaca s učinkovitom administrativnom i sudskom zaštitom, uključujući naknadu štete.

132. Korejski sustav osim toga nudi alternativne mehanizme kojima se pojedinci mogu poslužiti radi dobivanja pravne zaštite, uz administrativne i sudske načine, kako je objašnjeno u uvodnim izjavama 132. i 133. nacrta odluke, koje se odnose na pozivni centar za privatnost i odbor za posredovanje u sporovima. S obzirom na to da su ovo dodatni načini pravne zaštite, EDPB bi pozdravio detaljnija objašnjenja o tome kako nadopunjuju mogućnosti pravne zaštite prije PIPC-a i sudova za ispitanike čiji se osobni podatci prenose u Koreju prema odluci o primjerenosti.

[57] Vidjeti uvodnu izjavu 117. nacrta odluke i članak 62. Provedbenog dekreta.

4. PRISTUP I UPOTREBA OSOBNIH PODATAKA PRENESENIH IZ EUROPSKE UNIJE PREKO JAVNIH TIJELA U JUŽNU KOREJU

133. Kad je riječ o procjeni razine zaštite u područjima izvršavanja zakonodavstva i nacionalne sigurnosti, Europska komisija dala je detaljne informacije u nacrtu odluke i prilozima stavljenima na raspolaganje. Stoga je EDPB suzdržan glede ponavljanja većine činjeničnih stanja i procjena u ovom mišljenju.

134. Europska komisija došla je do zaključka da u prethodno navedenim područjima postoji razina zaštite koja odgovara zahtjevima određenim sudskom praksom Suda Europske unije te se stoga može smatrati u načelu istovjetnom onoj Europske unije.

135. Kao opću napomenu, EDPB bi želio naglasiti da čak i ako se čini ili Europska komisija tvrdi da se na podatke prenesene iz EU-a u Južnu Koreju vjerojatno neće primjenjivati relevantni korejski zakon, ipak je potrebno procijeniti primjerenost korejske razine zaštite podataka s obzirom na takve slučajeve. Njihova važnost dokazana je i činjenicom da ih je Europska komisija spomenula u nacrtu odluke.

4.1. Opći okvir zaštite podataka u kontekstu pristupa vlade

136. Kad je riječ o pristupu javnih tijela osobnim podatcima, potrebno je proučiti različite korejske zakone kako bi se procijenila razina zaštite prava na privatnost i zaštitu podataka. Prvo, EDPB ističe da PIPA, kao ključan zakon zaštite podataka, ima široku primjenu. Međutim, PIPA je u cijelosti primjenjiva na područje izvršavanja zakonodavstva, no njezina je primjena na obradu podataka radi nacionalne sigurnosti ograničena. Prema članku 58. stavku 1. točki 2. PIPA-e, Poglavlja III. do VII. ne primjenjuju se na obradu osobnih podataka radi nacionalne sigurnosti. Međutim, Poglavlja I., II., IX. i X. ostaju primjenjiva za područje nacionalne sigurnosti. Stoga se temeljna načela PIPA-e kao i temeljna jamstva za prava ispitanika i odredbe o nadzoru, izvršenju i pravnim lijekovima ne primjenjuju na pristup i upotrebu osobnih podataka od strane nacionalnih sigurnosnih tijelâ.

137. I Ustav Južne Koreje sadržava temeljna načela zaštite podataka, i to načela zakonitosti, nužnosti i proporcionalnosti. Ta su načela primjenjiva i na pristup osobnim podatcima koji javna tijela iz Južne Koreje imaju u području izvršavanja zakonodavstva i nacionalne sigurnosti[58].

138. U području izvršavanja zakonodavstva policija, tužitelji, sudovi i druga javna tijela mogu prikupljati osobne podatke na temelju posebnog zakonodavstva, odnosno Zakona o kaznenom postupku („**CPA**“), Zakona o zaštiti privatnosti komunikacija („**CPPA**“), Zakona o telekomunikacijskom poslovanju („**TBA**“) i Zakona o prijavi i upotrebi određenih podataka o financijskim transakcijama („**ARUSFTI**“), koji se primjenjuju na progon i prevenciju pranja novca i financiranje terorista. Ti određeni zakoni određuju dodatna ograničenja, zaštitne mjere i izuzeća.

139. U području nacionalne sigurnosti, na temelju Zakona o nacionalnoj obavještajnoj službi („**NISA**“) i dodatnih „nacionalnih sigurnosnih zakona”[59], Nacionalna obavještajna služba („**NIS**“) može prikupljati osobne podatke i presretati komunikacije. EDPB shvaća da NIS pri izvršavanju svojih ovlasti mora poštovati prethodno spomenute zakonske odredbe kao i PIPA-u.

140. EDPB od Komisije traži objašnjenje o tome postoje li druga tijela u Koreji, osim NIS-a, koja su odgovorna za područje nacionalne sigurnosti jer u odjeljku 6. Priloga I. Europska Komisija ostavlja dojam da je NIS primjer agencije za nacionalnu sigurnost.

[58] Vidjeti uvodnu izjavu 145. nacrta odluke.

[59] Nacionalni sigurnosni zakoni uključuju, primjerice, Zakon o zaštiti privatnosti komunikacija, Zakon protiv terorizma radi zaštite građana i javne sigurnosti ili Zakon o telekomunikacijskom poslovanju.

4.2. Zaštita i zaštitne mjere podataka o potvrdi komunikacije u kontekstu pristupa vlade za potrebe izvršavanja zakonodavstva

141. Na temelju mjerodavnog zakona, CPPA, tijela za izvršavanje zakonodavstva mogla bi primijeniti dvije vrste mjera za procjenu komunikacijskih podataka. CPPA razlikuje mjere ograničavanja komunikacija koje obuhvaćaju prikupljanje sadržaja uobičajene pošte i izravno presretanje sadržaja telekomunikacija[60] te prikupljanje takozvanih podataka o potvrdi komunikacije. Potonji uključuju datum telekomunikacija, vrijeme početka i završetka, broj izlaznih i dolazni poziva kao i broj pretplatnika druge strane, učestalost upotrebe, datoteke dnevnika o upotrebi telekomunikacijskih usluga i podatke o lokaciji[61].

142. EDPB ističe da podatci o potvrdi komunikacije nemaju jednake zaštitne mjere kao podatci prikupljeni putem mjera za ograničavanje komunikacije, odnosno podataka o sadržaju. Zaista, EDPB ističe da prikupljanje sadržaja ima veće zaštitne mjere od prikupljanje podataka o potvrdi komunikacije za potrebe izvršavanja zakonodavstva: Prvo, za razliku od prikupljanja podataka o sadržaju, prikupljanje podataka o potvrdi komunikacije nije ograničeno na istraživanje određenih ozbiljnih kaznenih dijela, nego se može provoditi kad se smatra potrebnim za provođenje „svakog istraživanja ili izvršenja bilo koje kazne“ (članak 13. stavak 1. CPPA-e). Drugo, prikupljanje podataka o potvrdi komunikacije u načelu nije strukturirano kao krajnja mjera i za upotrebu samo ako je na drugi način teško spriječiti počinjenje kaznenog dijela, uhititi počinitelja ili prikupiti dokaze[62]. Podatci o potvrdi komunikacije mogu se prikupljati kad god tužitelj ili pravosudni policijski službenik to „smatra nužnim“ za istraživanje kaznenog djela ili izvršavanje kazne. Međutim, postoji izuzeće s obzirom na ove podatke praćenja u stvarnom vremenu i podatke o potvrdi komunikacije za određenu osnovnu postaju u skladu s člankom 13. stavkom 2. CPPA-e. Treće, tijela za izvršavanja zakonodavstva koja prikupljaju sadržaj komunikacije odmah moraju prestati s time kad se trajni pristup više ne smatra nužnim[63]. S obzirom na podatke o potvrdi komunikacije, to nije izričito navedeno u CPPA-i ili njezinu Provedbenom dekretu.

143. EDPB ističe da se prikupljanje podataka o potvrdi komunikacije smije provesti samo na temelju sudskog naloga. Štoviše, CPPA traži detaljne informacije u zahtjevu naloga i u samom nalogu[64]. Takvo prethodno sudsko odobrenje služi ograničavanju diskrecije tijelâ za izvršavanje zakonodavstva u primjeni zakona i za provjeru postoje li u svakom slučaju dovoljni razlozi za prikupljanje podataka o potvrdi komunikacije. EDPB ujedno prepoznaje da zakon Republike Koreje vjerojatno ne predviđa opće i neselektivno zadržavanje podataka o potvrdi komunikacije. Stoga se pristup vlade takvim podatcima uvijek povezuje s podatcima koji su još zadržani radi naplate i pružanja samih komunikacijskih usluga.

144. Međutim, EDPB naglašava da je Sud Europske Unije doveo u pitanje činjenicu da su podatci o prometu manje osjetljivi od drugih, a posebice od podataka sadržaja[65]. Uzimajući u obzir da se podatcima o potvrdi komunikacije daje manja razina zaštite nego podatcima sadržaja u nekoliko aspekata, EDPB poziva Europsku komisiju na pomno praćenje jamče li zaštitne mjere osigurane korejskim pravom za

[60] Članak 3. stavak 2., članak 2. stavak 6., članak 2. stavak 7. CPPA-e.
[61] Članak 2. stavak 11. CPPA-e.
[62] To je slučaj podataka sadržaja u skladu s člankom 3. stavkom 2. i člankom 5. stavkom 1. CPPA-e.
[63] Članak 2. Provedbenog dekreta CPPA-e.
[64] Vidjeti uvodnu izjavu 156. nacrta odluke.
[65] Vidjeti Sud Europske unije, C-623/17, *Privacy International,* 6. listopada 2020., ECLI:EU:C:2020:790, t. 71.: *„Miješanje prijenosa podataka o prometu i lokaciji sigurnosnim i obavještajnim službama u pravo utvrđeno člankom 7. Povelje treba smatrati osobito ozbiljnim, uzimajući u obzir, među ostalim, osjetljivost informacija koje mogu pružiti te podatke, a osobito mogućnost da se na temelju njih utvrdi profil predmetnih osoba, što je jednako osjetljiva informacija kao i sam sadržaj komunikacija. Ono usto može kod predmetnih osoba stvoriti osjećaj da je njihov privatni život predmet trajnog nadzora (vidjeti po analogiji presude od 8. travnja 2014., Digital Rights Ireland and Others., C‑293/12 i C‑594/12, EU:C:2014:238, t. 27. i 37., i od 21. prosinca 2016., Tele2, C‑203/15 i C‑698/15, EU:C:2016:970, t. 99. i 100.).“*

takve kategorije osobnih podataka u načelu istovjetnu razinu zaštite onoj zajamčenoj u EU-u, posebice za proporcionalnost i predvidljivost zakona.

4.3. Pristup korejskih javnih tijela komunikacijskim podatcima radi nacionalne sigurnosti

145. S obzirom na pravni okvir za pristup nacionalnih sigurnosnih tijelâ komunikacijskim podatcima prenesenima iz EGP-a u Koreju, EDPB je prepoznao dva razloga za zabrinutost, a oba su povezana s režimom pristupa komunikacijama među onima koji nisu korejski državljani, a koji pripadaju određenim slučajevima upotrebe (vidjeti t. 29.). U tim slučajevima, s obzirom na podatke o potvrdi komunikacije i sadržajne podatke, ne primjenjuju se određene zaštitne mjere koje su inače predviđene. Drugim riječima, u tim određenim slučajevima, ti podatci nemaju jednake zaštitne mjere kao podatci o kojima se obavještava kad je u komunikaciju uključen najmanje jedan korejski državljanin.

4.3.1. Nema obveze obavještavanja pojedinaca o pristupu vlade komunikaciji između stranih državljana

146. U prethodno opisanom scenariju, odnosno ako nijedna strana komunikacije nije korejski državljanin, tijela nacionalne sigurnosti nisu obvezne obavijestiti pojedince o prikupljanju i obradi njihovih podataka. EDPB prepoznaje da ovaj problem utječe samo na određene slučajeve. Prvo, kako je već navedeno, kad je u komunikaciju uključen najmanje jedan korejski državljanin, zahtjevi za obavješćivanje u skladu s CPPA-om primjenjuju se na sve strane komunikacije bez obzira na njihovo državljanstvo[66]. Drugo, za prikupljanje osobnih podataka koji proizlaze iz komunikacija isključivo između stranih državljana vrijede posebni slučajevi uporabe. Konkretno, pravo pristupa posebice u takvim slučajevima obuhvaća komunikacije a) zemalja protivnica Republici Koreji, b) stranih agencija, skupina ili državljana za koje se sumnja da provode aktivnosti protiv Koreje[67], ili c) članova skupina koje rade unutar korejskog poluotoka, ali učinkovito izvan suvereniteta Republike Koreje i njihovih krovnih skupina sa sjedištem u stranima državama. Stoga se komunikacije između pojedinaca iz EU-a koje se prenose iz EGP-a u Koreju mogu prikupljati samo radi nacionalne sigurnosti ako pripadaju jednoj od tri prethodno navedene kategorije[68]. Kao dodatni ograničavajući faktor, EDPB je iz dodatnih objašnjenja Europske komisije shvatio da primjenjivi pravni okvir ne omogućuje presretanje podataka u tranzitu izvan Koreje.

147. Stoga bi se kritičnost nedostatka zahtjeva za obavješćivanje, u okvirima praktičnog utjecaja, mogla smatrati ograničenom. Međutim, EDPB naglašava važnost (naknadne) obavijesti o pristupu vlade, posebice za jamstvo djelotvornog pravnog lijeka. Prema Sudu Europske unije, „*obavijest je potrebna da se tim osobama omogući da se koriste svojim pravima koja proizlaze iz članaka 7. i 8. Povelje, da zahtijevaju pristup svojim osobnim podatcima koji su predmet tih mjera te, po potrebi, njihov ispravak ili brisanje, kao i da, u skladu s člankom 47. prvim stavkom Povelje, podnesu djelotvoran pravni lijek pred sudom*”[69]. Pristup vlade radi nacionalne sigurnosti često uključuje tajne mjere nadzora, što znači da ciljevi nadzora, odnosno ispitanici, nisu svjesni obrade njihovih podataka. Stoga, „*u načelu nema dovoljno prostora da dotični pojedinac pribjegne sudovima osim ako se tom pojedincu ne savjetuje o mjerama poduzetima bez njegova znanja i ako on samim tim može retrospektivno osporiti njihovu zakonitost ili, alternativno, osim ako svaka osoba koja sumnja da su njegove komunikacije presretnute*

[66] Vidjeti uvodnu izjavu 192. nacrta odluke.
[67] Vidjeti Prilog II., bilješka 244., u skladu s kojim se pojam aktivnosti protiv Koreje odnosi na aktivnosti koje prijete nacionalnom postojanju i sigurnosti, demokratskom poretku ili preživljavanju i slobodi ljudi.
[68] Vidjeti uvodnu izjavu 187. nacrta odluke.
[69] Sud Europske unije, spojeni predmeti C-511/18, C-512/18 i C-520/18, *La Quadrature du Net i ostali,* 6. listopada 2020., ECLI:EU:C:2020:791, t. 190.

ili su bile presretnute ima pravo na djelotvoran pravni lijek, tako da nadležnost sudova ne ovisi o obavijesti subjektu presretanja da je došlo do presretanja njegovih komunikacija."[70] U tom kontekstu i dosljedno ovome, EDPB mnogo je puta izrazio svoju zabrinutost za djelotvoran pravni lijek u slučajevima nadzora. EDPB naglašava da posljedica tajnovitosti mjera vlade ne smije biti učinkovito neosporavanje takvih mjera. S time u vezi, utječe li nedostatak zahtjeva za obavješćivanje za komunikacije između stranih državljana na razinu zaštite podataka kako je procijenjeno u nacrtu odluke mora se procijeniti kao dio ukupne procjene uz posebnu napomenu na mehanizme nadzora i pravne zaštite koje pruža korejski zakon (vidjeti odjeljke 4.7. i 4.8.).

148. EDPB dodatno u ovom kontekstu ističe da se zakon odnosi na šire pojmove kao što je aktivnosti protiv Koreje ili protiv države[71] te da je teško predvidjeti kako su ovi koncepti konstruirani prema korejskom zakonu. EDPB poziva Europsku komisiju da prati razradu ovih u korejskom zakonu te odgovara li njihova primjena u praksi zahtjevima proporcionalnosti prema pravu EU-a.

4.3.2. Nema prethodnog neovisnog odobrenja za prikupljanje komunikacijskih podataka između stranih državljana

149. Ako se osobni podatci EGP-a dobiveni iz komunikacije između osoba koje nisu korejski državljani (te pripadaju u jednu od prethodno navedenih slučajeva upotrebe) obrađuju u Koreji radi nacionalne sigurnosti, prikupljanje takvih podataka nije predmet prethodnog odobrenja neovisnog tijela (kao što je slučaj za komunikacije ako je najmanje jedan od pojedinaca korejski državljanin)[72].

150. Posebice s obzirom na nedavne odluke Europskog suda za ljudska prava („**ECtHR**"), „Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva" i „Centrum för Rättvisa protiv Švedske", EDPB smatra da je nužno istražiti je li to kritični nedostatak korejskog okvira za zaštitu podataka. EDPB podsjeća da, kako je istaknuto u ažuriranim preporukama za Europska temeljna jamstva za mjere nadzora[73], članak 6. stavak 3. Ugovora o Europskoj uniji navodi da temeljna prava utvrđena na Europskom sudu za ljudska prava sadržavaju osnovna načela prava EU-a dok, kako Sud Europske unije podsjeća u svojoj sudskoj praksi, potonje ne čini, sve dok mu Europska unija nije pristupila, zakonski instrument koji je formalno ugrađen u pravo EU-a[74]. Stoga se razina zaštite temeljnih prava potrebna prema članku 45. Opće uredbe mora utvrditi na temelju odredbi te Uredbe, u smislu temeljnih prava sadržanih u Povelji. Prema tome, u skladu s člankom 52. stavkom 3. Povelje o pravima utvrđenima u njoj, koji odgovaraju pravima koje jamči Europski sud za ljudska prava, moraju imati jednako značenje i područje primjene kao ona utvrđena Konvencijom. Posljedično tome, sudska praksa Europskog suda za ljudska prava koja se odnosi na prava predviđena i u Povelji mora se uzeti u obzir kao najmanji prag zaštite za tumačenje odgovarajućih prava u Povelji, odnosno u mjeri da Povelja, kako je tumači Sud Europske unije, ne pruža veću razinu zaštite[75].

151. EDPB ističe da, bez obzira na to što se prethodno (neovisno) odobrenje mjera nadzora smatra važnom zaštitnom mjerom protiv arbitrarnosti, takvo odobrenje ne može se izvesti iz sudske prakse Suda

[70] ECtHR, *Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva*, 25. ožujka 2021., ECLI:CE:ECHR:2021:0525JUD005817013, t. 337. i ECtHR, *Predmet Roman Zakharov protiv Rusije*, 4. prosinca 2015., ECLI:CE:ECHR:2015:1204JUD004714306, t. 234.

[71] Europska komisija je objasnila da se to, prema objašnjenjima korejske vlade, odnosi na „aktivnosti koje prijete nacionalnom postojanju i sigurnosti, demokratskom poretku ili preživljavanju i slobodi ljudi", vidjeti i bilješku 319. nacrta odluke o primjerenosti.

[72] Vidjeti uvodnu izjavu 190. nacrta odluke.

[73] Vidjeti Preporuke 02/2020 o europskim temeljnim jamstvima za mjere nadzora EDPB-a, t. 10., 11.

[74] Vidjeti Sud Europske unije, C-311/18, *Povjerenik za zaštitu podataka protiv subjekata Facebook Ireland Ltd i Maximillian Schrems*, 16. srpnja 2020., ECLI:EU:C:2020:559 (dalje u tekstu„*Schrems II*"), t. 98.

[75] Vidjeti Sud Europske unije, spojeni predmeti C-511/18, C-512/18 i C-520/18, *La Quadrature du Net and others*, 6. listopada 2020., t. 124.

Europske unije kao apsolutno potrebno za proporcionalnost mjera nadzora. Međutim, Europski sud za ljudska prava sada je izričito utvrdio zahtjeve za *ex ante* neovisno odobrenje masovnog presretanja[76]. Nacrt odluke ne navodi to izričito, ali EDPB razumije da pravni okvir Republike Koreje ne predviđa masovno presretanje, nego samo ciljano presretanje telekomunikacija[77]. Europska komisija potvrdila je ovo razumijevanje.

152. Prema tome, prethodno navedene odluke Europskog suda za ljudska prava, sukladno sudskoj praksi Suda Europske unije[78] i prethodnim sudskim praksama Europskog suda za ljudska prava[79], ponovno pokazuju važnost sveobuhvatnog nadzora neovisnih nadzornih tijela. EDPB naglašava da je neovisan nadzor na svim razinama postupka pristupa vlade za potrebe izvršavanja zakonodavstva i nacionalne sigurnosti važna zaštitna mjera protiv arbitrarnih mjera nadzora te tako i za procjenu primjerene razine zaštite podataka. Svrha jamstva neovisnosti nadzornih tijela prema značenju članka 8. stavka 3. Povelje je osigurati učinkovito i pouzdano praćenje poštivanja pravila o zaštiti pojedinaca u vezi s obradom osobnih podataka. To se posebice odnosi na okolnosti u kojima je, zbog prirode tajnog nadzora, pojedincu onemogućeno traženje revizije ili neposredno sudjelovanje u bilo kakvim postupcima revizije prije ili tijekom provedbe mjere nadzora.

153. Nedostatak prethodnog neovisnog odobrenja ne može se sam smatrati značajnim nedostatkom u korejskom zakonu s obzirom na procjenu u načelu istovjetne razine zaštite podataka. Procjena primjerenosti ponovno ovisi o svim okolnostima slučaja, posebice o učinkovitosti *ex post* nadzora i pravne zaštite kako je predviđeno u pravnom okviru Koreje (vidjeti daljnje odjeljke 4.7. i 4.8.).

4.4. Dobrovoljna objavljivanja

154. Prema članku 83. stavku 3. TBA-e, pružatelji telekomunikacijskih usluga mogu dobrovoljno na zahtjev predati takozvane „podatke pretplatnika“[80] tijelima nacionalne sigurnosti i tijelima za izvršavanje zakonodavstva. EDPB ističe da slučajevi koji uključuju osobne podatke koji su preneseni iz EGP-a u Koreju vjerojatno rijetki, svejedno se moraju analizirati kako bi se procijenila razina zaštite podataka, kako je prethodno već navedeno.

155. EDBP razumije da se u tim slučajevima zaštitne mjere podataka PIPA-e primjenjuju te da javna tijela, kao i pružatelji telekomunikacijskih usluga, moraju ispunjavati te zahtjeve[81] te da se i jedni i drugi mogu smatrati odgovornima za bilo kakvo kršenje prava i sloboda dotičnih ispitanika[82]. Nadalje, EDPB razumije da pružatelji telekomunikacijskih usluga ne moraju ispunjavati takve zahtjeve.

---

[76] Vidjeti Europski sud za ljudska prava, *Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva*, 25. svibnja 2021., ECLI:CE:ECHR:2021:0525JUD005817013, t. 351.: „Masovno presretanje trebalo bi najprije biti predmet neovisnog odobrenja“, „masovno presretanje trebalo bi odobriti neovisno tijelo, odnosno tijelo koje je neovisno o izvršnoj vlasti“.

[77] Samo Prilog II., odjeljak 3.2. sadržava izričitu deklaraciju radi nacionalne sigurnosti gdje je navedeno da ograničenja zaštitnih mjera *„jamče da su prikupljanje i obrada podataka ograničeni na ono što je uistinu nužno za postizanje legitimnog cilja*. *To isključuje svako masovno i neselektivno prikupljanje osobnih podataka radi nacionalne sigurnosti*“.

[78] Vidjeti, primjerice, Sud Europske unije, povezani predmeti C-203/15 i C-698/15, *Tele2 Sverige AB and others*, ECLI:EU:C:2016:970.

[79] Vidjeti, primjerice, Europski sud za ljudska prava, *Predmet Roman Zakharov protiv Rusije*, 4. prosinca 2015., ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Skupovi podataka na koje se ovo odnosi bili bi: ime i prezime, matični broj stanovnika, adresa i broj telefona korisnika, datumi na koje se korisnici pretplaćuju ili otkazuju pretplatu te njihove identifikacijske kodove korisnika (koji se upotrebljavaju za identifikaciju zakonitog korisnika računalnih sustava ili komunikacijskih mreža).

[81] Vidjeti uvodnu izjavu 164. i 194. nacrta odluke.

[82] Vidjeti uvodnu izjavu 166. nacrta odluke.

156. Međutim, s obzirom na koncept pristupa nacionalnih tijela podatcima pretplatnika radi izvršavanja zakonodavstva, a posebice radi nacionalne sigurnosti putem „dobrovoljnog objavljivanja“ telekomunikacijskih poslovnih operatera, postoji zabrinutost za povećani rizik za prava i slobode ispitanika, posebice za njihovo pravo na informacije.

157. Prema članku 58. stavku 1. točki 2. PIPA-e, odredbe Poglavlja III. do VII. ne odnose se na osobne podatke koji su zatraženi radi nacionalne sigurnosti. Prema tome, primjerice, odredbe članka 18. (ograničenje upotrebe bez svrhe i davanje osobnih podataka) i članka 20. (obavijest o izvorima itd. osobnih podataka prikupljenih od trećih strana) PIPA-e ne primjenjuju se za takve zahtjeve. Ako tijelo nacionalne sigurnosti podnese zahtjev, postavlja se pitanje, s jedne strane, isključuje li članak 58. stavak 1. točka 2. primjenu PIPA-e i za pružatelje telekomunikacijskih usluga. S druge se strane postavlja pitanje primjenjuje li se izuzeće primjene članka 20. PIPA-e u takvim slučajevima i na odgovarajuću odredbu iz odjeljka 3. Priloga I. (Obavijest za podatke ako osobni podatci nisu dobiveni od ispitanika (članak 20. Zakona)). Ako je to slučaj i ako se članak 58. stavak 1. točka 2. odnosi i na pružatelje telekomunikacijskih usluga, postojao bi rizik, u skladu s dostupnim podatcima, od nepostojanja zakonske obveze za obavještavanjem ispitanika o dobrovoljnom objavljivanju.

158. EDPB je stoga zabrinut za učinkovitost, odnosno da bi zahtjevi za podatcima postali neučinkoviti i tako ispitanicima otežali ostvarivanje prava na zaštitu podataka, posebice za sudsku zaštitu. Prema tome, EDPB poziva Europsku komisiju da razjasni područje primjene relevantnih odredbi.

1.5. Daljnja upotreba podataka

159. Načelo ograničenja svrhe temeljni je pravni zahtjev za zaštitu podataka. Zahtijeva da se osobni podatci prikupljaju samo u određene, izričite i legitimne svrhe te da se ne obrađuju dalje na način koji nije u skladu s tim svrhama. Nadalje, prema pravu EU-a javna tijela smiju obrađivati osobne podatke radi sprječavanja, istraživanja ili progona kaznenih djela čak i ako su ti podatci prvenstveno prikupljeni u druge svrhe ako ta tijela imaju pravni temelj za obradu takvih podataka prema primjenjivom zakonu i ako daljnja obrada nije ne proporcionalna[83].

160. Prema ovome, EDPB ističe da korejski okvir za zaštitu podataka predviđa zaštitne mjere i ograničenja slične onima predviđenima u pravu EU-a u vezi s daljnjom uporabom podataka prikupljenih radi izvršavanja zakonodavstva i nacionalne sigurnosti, npr. načelo ograničenja svrhe iz članka 3. stavaka 1. – 2. PIPA-e, .

1.6. Daljnji prijenosi i razmjena obavještajnih podataka

161. Članak 44. Opće uredbe o zaštiti podataka navodi da se prijenosi i daljnji prijenosi osobnih podataka smiju provoditi samo ako razina zaštite zajamčena Općom uredbom o zaštiti podataka nije ugrožena. Stoga se razina zaštite pružena osobnim podatcima prenesenima iz EGP-a u Koreju ne smije ugrožavati daljnjim prijenosima primateljima u trećoj zemlji, odnosno daljnji prijenosi trebali bi biti dozvoljeni samo je osigurana neprekidna razina zaštite u načelu istovjetna onoj pruženoj prema pravu EU-a. Posljedično, kad se procjenjuje jamči li treća zemlja primjerenu razinu zaštite podataka, mora se uzeti u obzir pravni okvir zemlje za daljnje prijenose. To je neporecivo i u skladu sa stavovima Europske unije[84] i EDPB-a.

162. U ovom kontekstu, EDPB ističe da je Europski sud za ljudska prava u svojim nedavnim odlukama „Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva“ i „Centrum för Rättvisa protiv Švedske“ dao

[83] Vidjeti članak 4. stavak 2. Direktive o izvršavanju zakonodavstva.
[84] Vidjeti uvodnu izjavu 84. i dalje u nacrtu odluke.

smjernice[85] za mjere predostrožnosti zaštite podataka koje se moraju poštivati u ugovornim državama kad se o osobnim podatcima obavještavaju druge strane radi izvršavanja zakonodavstva i radi nacionalne sigurnosti u slučajevima skupnog prikupljanja: „*Prvo, okolnosti u kojima može doći do ovakvog prijenosa moraju izričito biti navedene u nacionalnim zakonima*. *Drugo, država koja prenosi mora osigurati da država koja prima, pri rukovanju podatcima, ima uspostavljene zaštitne mjere sposobne za sprječavanje zlouporabe i nerazmjernog zadiranja. Država koja prima posebice mora jamčiti sigurnu pohranu materijala i ograničiti daljnje objavljivanje.* […] *Treće, povećane zaštitne mjere bit će nužne kad je jasno da se prenosi materijal za koji je potrebna posebna povjerljivost, kao što je povjerljiv novinarski materijal*.“[86]

163. Primjenom ovih standarda, Europski sud za ljudska prava u predmetu „Centrum för Rättvisa protiv Švedske“ zaključio je da nedostatak izričitog pravnog zahtjeva za režim presretanja radi procjene nužnosti i proporcionalnosti mogućeg utjecaja razmjene obavještajnih podataka na pravo na privatnost predstavlja kršenje članka 8. Europske konvencije o ljudskim pravima. Europski sud za ljudska prava kritizirao je da bi se, kao rezultat općenite razine zakona, presretnuti materijal općenito morao poslati u inozemstvo kad god se smatra da je to u nacionalnom interesu, bez obzira na to nudi li inozemni primatelj prihvatljivu najmanju razinu zaštitnih mjera[87].

164. Prihvaćanjem da pravni okvir Južne Koreje ne dozvoljava masovno presretanje, no na temelju implikacija sudske prakse Europskog suda za ljudska prava kako je prethodno navedeno, EDPB smatra da bi, uz zahtjeve koji proizlaze iz prava EU-a, a koje tumači Sud Europske unije, trebalo uzeti u obzir argumentaciju Europskog suda za ljudska prava da bi se procijenilo pruža li pravni okvir za daljnje prijenose trećoj zemlji primjerene standarde zaštite podataka.

4.6.1. Primjenjiv pravni okvir za daljnje prijenose tijela za izvršavanje zakonodavstva

165. Kad je riječ o daljnjem prijenosu nadležnih tijela u svrhu izvršavanja zakonodavstva, EDPB iz objašnjenja Europske komisije razumije da je odjeljak 2. Priloga I. nacrta odluke o ograničenju daljnjih prijenosa primjenjiv, među ostalim kad se prijenos provodi na temelju statuta koji nije PIPA. Prema tom pravilu, „*ako se osobni podatci prekomorski pruže trećoj strani, možda neće dobiti razinu zaštite koju jamči Zakon o zaštiti osobnih podataka Koreje zbog razlika sustava zaštite osobnih podataka različitih zemalja*. *Takvi će se slučajevi prema tome smatrati „slučajevima u kojima bi ispitanici mogli pretrpjeti štete“ , što je navedeno u članku 17. stavku 4. Zakona ili „slučajevima u kojima se nepravedno krše interes ispitanika ili treće strane“, što je navedeno u članku18. stavku 4. Zakona i članku 14. stavku 2. Provedbenog dekreta istog Zakona. Kako bi se ispunili zahtjevi ovih odredbi, voditelj obrade osobnih podataka i treća strana stoga moraju izričito osigurati razinu sigurnosti istovjetnu Zakonu, uključujući jamstvo ostvarivanja prava ispitanika u pravno obvezujućim dokumentima kao što su ugovori, čak i nakon prekomorskog prijenosa osobnih podataka“*[88].

166. EDPB pozdravlja ovu odredbu koja, uz pretpostavku primjerenosti razine zaštite podataka u Koreji za ovu svrhu, osigurava nastavak razine zaštite kakva je načelno pružena prema pravu EU-a za daljnje prijenose. Komisija je potvrdila da je EDPB točno razumio da se ovaj odjeljak Priloga I. odnosi na sve

[85] Sljedeći su elementi uspostavljani za vrijeme trajanja predmeta *Big Brother Watch* i *Centrum för Rättvisa* koji se odnose na režime masovnog presretanja. Zahtjev za poduzimanje mjera predostrožnosti pri prijenosu materijala drugim stranama već je bio dijelom kriterija koji je razvio Europski sud za ljudska prava u kontekstu ciljanog presretanja te ga Europski sud za ljudska prava nije podrobnije utvrdio (vidjeti *Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva*, t. 335., 362.).

[86] Europski sud za ljudska prava, *Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva*, 25. svibnja 2021., ECLI:CE:ECHR:2021:0525JUD005817013, t. 362.

[87] Vidjeti Europski sud za ljudska prava, *Centrum för Rättvisa protiv Švedske*, 25. svibnja 2021., ECLI:CE:ECHR:2021:0525JUD003525208, t. 326.

[88] Nacrt odluke, Prilog I., str. 7.

daljnje prijenose nadležnih tijela radi izvršavanja zakonodavstva. Međutim, EDPB naglašava da se mora osigurati da ovo pravilo pruža neprekidnu razinu zaštite u praksi jer bi mogla postojati nesigurnost oko toga koje se ugovorne zaštitne mjere i obveze ili drugi slični mehanizmi smiju upotrebljavati za postizanje te razine zaštite u slučaju obrade u svrhu izvršavanja zakonodavstva. U tom pogledu trebalo bi se dodatno navesti, primjerice, da se osobni podatci smiju dijeliti samo s relevantnim nadležnim tijelima u trećoj zemlji.

167. Predmet prethodno zatraženog pojašnjenja o tome pripada li KOFIU nacrtu odluke, EDPB ističe da službena izjava o pristupu vlade[89] objašnjava da bi, prema članku 8. stavku 1. ARUSFTI-a, povjerenik KOFIU-a inozemnim financijskim obavještajnim službama mogao dati određene podatke o financijskim transakcijama ako se to smatra potrebnim za ostvarivanje svrhe ARUSFTI-a[90]. Sam članak 8. ARUSFTI-a ne predviđa obvezu za određivanje nudi li strana zemlja primjerene zaštitne mjere podataka te jamči li ih. Prilog II. ne odnosi se na novi odjeljak Priloga I. EDPB stoga poziva Europsku komisiju da razjasni međusobne odnose relevantnih odjeljaka Priloga I. o ograničenju daljnjih prijenosa i pravne osnove za daljnje prijenose prema ARUSFTI-u.

4.6.2. Primjenjiv pravni okvir za daljnje prijenose radi nacionalne sigurnosti

168. Nacrt odluke ne sadržava nikakve informacije o pravnom okviru za daljnje prijenose u području nacionalne sigurnosti. Zbog toga EDPB razumije da, za razliku od svrhe izvršavanja zakonodavstva, odjeljak 2. Priloga I. nije primjenjiv na daljnje prijenose radi nacionalne sigurnosti. Članci 17. i 18. PIPA-e, koji su predmeti Priloga I. dotičnog odjeljka, dio su Poglavlja III. PIPA-e koji u konačnici nije primjenjiv na obradu osobnih podataka radi nacionalne sigurnosti (članak 58. stavak 1. PIPA-e).

169. Međutim, EDPB pretpostavlja da Koreja ne treba i ne prenosi osobne podatke stranim obavještajnim službama radi nacionalne sigurnosti, npr. radi suradnje u borbi protiv prekograničnih prijetnji nacionalnoj sigurnosti, kako bi se upozorile strane vlade o njima ili radi traženja pomoći u identifikaciji takvih prijetnji.

170. EDPB je shvatio da su, prema Europskoj komisiji, daljnji prijenosi u korejskom zakonu dovoljno regulirani zaštitnim mjerama koje su izvedene iz sveobuhvatnog ustavnog okvira, posebice načela nužnosti i proporcionalnosti, kao i temeljnim načelima zaštite podataka koje regulira PIPA kao što je zakonitost i pravednost obrade, ograničavanje svrhe, smanjenje količine podataka, sigurnost i opća obveza sprječavanja zlouporabe i nepravilne uporabe osobnih podataka.

171. EDPB prepoznaje i prihvaća opću primjenjivost ovih ključnih načela (zaštite podataka), ali izražava zabrinutost da su te zaštitne mjere vrlo općenite prirode i ne odnose se specifično, na pravnoj osnovi, na određene okolnosti i uvjete za daljnji prijenos prenesenih podataka EGP-a radi nacionalne sigurnosti. Iako su ova opća i sveobuhvatna načela široko primjenjiva, EDPB razmatra može li se smatrati da to ispunjava kriterije jasnih i preciznih pravila te da dovoljno utvrđuje učinkovite i primjenjive zaštitne mjere. Posebice ako se pristup vlade i obrada osobnih podataka provodi u tajnosti, a zaključci koji bi mogli proizaći iz podataka posebno su ozbiljni, važno je imati jasna, detaljna pravila. Zakon bi trebao dovoljno jasno navesti razmjere diskrecije dodijeljene nadležnim tijelima i način njihova izvršavanja kako bi pojedincu pružio primjerenu zaštitu. U presudi *Schrems II*, Sud Europske unije podsjeća da pravna osnova koja dozvoljava zadiranje u temeljna prava mora i sama, kako bi zadovoljila zahtjeve načela nužnosti i proporcionalnost, definirati razmjer ograničenja izvršenja

[89] Vidjeti nacrt odluke, Prilog II.

[90] Vidjeti nacrt odluke, Prilog II., odjeljak 2.2.3.2. S obzirom na to da se takva razmjena smije provesti samo podložno uvjetima da strana služba ne smije upotrijebiti podatke u bilo koju svrhu osim izvorne svrhe objavljivanja, a posebice ne za kaznenu istragu ili suđenje (članak 8. stavak 2. ARUSFTI-a), povjerenik KOFIU-a može, po primitku zahtjeva strane zemlje, dati privolu za upotrebu tih podataka radi kaznene istrage ili suđenja za kaznena djela uz prethodnu privolu Ministra pravosuđa (članak 8. stavak 3. ARUSFTI-a).

dotičnog prava te utvrditi jasna i precizna pravila koja određuju područje i primjenu dotične mjere i propisati minimalne zaštitne mjere[91]. EDPB je stoga zabrinut da nije dovoljno da su takve zaštitne mjere općenito sadržane u nadređenom pravu bez izričitog uvrštenja pojma, npr. proporcionalnosti, u predmetnu pravnu osnovu.

172. Ove dvojbe potvrđuje prethodno navedena odluka Europskog suda za ljudska prava u kojoj je sud odlučio da opće pravilo bez izričitog zahtjeva za procjenu nužnosti i proporcionalnosti ili uzimanje u obzir pitanja privatnosti nije u skladu s pravom na privatnost u skladu s člankom 8. Europske konvencije o ljudskim pravima. U tom pogledu, EDPB ističe da u zakonu dotičnog predmeta (kao i u korejskom zakonu), sveobuhvatna (jamčena ustavom) načela nužnosti i proporcionalnosti zaista postoje, primjerice prema Povelji i pristupom Europskoj konvenciji o ljudskim pravima.

173. EDPB poziva Europsku komisiju na pojašnjenje pravne osnove, na koji način i u kojoj mjeri te pod kojim određenim uvjetima obavještajne službe imaju obvezu uzeti u obzir zabrinutosti za privatnost i zaštitne mjere podataka prije objavljivanja osobnih podataka stranim partnerima radi nacionalne sigurnosti. Ako se ta obveza izvede izravno iz ustavnih načela, Europska komisija trebala bi dalje procijeniti zahtjeve preciznosti i jasnoće relevantnog zakona te potvrditi da se opća ustavna načela i načela zaštite podataka primjenjuju i provode na odgovarajući način.

4.6.3. Međunarodni sporazumi

174. U tom kontekstu EDPB ističe da Europska komisija nije, kao dio svoje procjene primjerenosti, uzela u obzir postojanje međunarodnih sporazuma sklopljenih između Koreje i trećih zemalja ili međunarodnih organizacija kojima bi se mogle predvidjeti specifične odredbe za međunarodni prijenos osobnih podataka službi za izvršavanje zakonodavstva i/ili obavještajnih službi trećim zemljama. EDPB smatra da će sklapanje bilateralnih ili multilateralnih sporazuma s trećim zemljama u svrhu izvršavanja zakonodavstva ili obavještajne suradnje vjerojatno utjecati na korejski pravni okvir zaštite podataka, kako je bilo procijenjeno.

175. Stoga EDPB poziva Europsku komisiju da objasni postoje li takvi sporazumi, pod kojim se uvjetima mogu sklopiti i mogu li odredbe međunarodnih sporazuma utjecati na razinu zaštite zajamčenu osobnim podatcima koji se prenose iz EGP-a u Koreju zakonskim okvirom i praksama povezanima s prekomorskim objavljivanjima radi izvršavanja zakonodavstva i nacionalne sigurnosti.

4.7. Nadzor

176. EDPB ističe da je nadzor tijela kaznenog progona kao i tijelâ nacionalne sigurnosti osiguran kombinacijom različitih unutarnjih i vanjskih tijela.

177. U ovom kontekstu je potrebno istaknuti da je Sud Europske unije opetovano naglasio potrebu za neovisnim nadzorom kao temeljnom komponentom zaštite fizičkih osoba s obzirom na obradu njihovih osobnih podataka. Koncept neovisnosti obuhvaća područja institucijske autonomije, slobode od primanja uputa i materijalne neovisnosti. Kako bi se osiguralo dosljedno praćenje i provedba zakona o zaštiti podataka, nadzorna tijela moraju imati učinkovite ovlasti, uključujući ovlasti za ispravljanje i ovlasti za preinaku.

178. EDPB se slaže sa zaključkom Europske komisije da se, u općenitoj procjeni, može smatrati da Koreja ima neovisan i učinkovit sustav nadzora, iako nekoliko tijela sustava nadzora sama ne ispunjavaju prethodno navedene zahtjeve. Primjerice, većina ih nema izvršne ovlasti, nego su ograničene samo na preporuke, primjerice Nacionalna komisija za ljudska prava ili Uprava za revizije i inspekcije. Nadalje, većina predmetnih državnih tijela nisu isključivo ustanove za zaštitu podataka, nego su im uglavnom povjereni drugi zadatci u području zaštite temeljnih prava.

[91] Vidjeti *Schrems II*, t. 175. i 180.

179. Međutim, prema objašnjenjima Europske komisije, EDPB ističe da PIPC sveobuhvatno i bez iznimke jamči nadzor tijelâ za izvršavanje zakonodavstva. Stoga PIPC ima ovlasti za istraživanje, ispravljanje i izvršavanje na temelju PIPA-e i drugih zakona za zaštitu podataka (npr. CPPA) koji se odnose na cijelo područje pristupa osobnim podatcima od strane tijel â za izvršavanja zakonodavstva i nacionalnu sigurnost.

180. U tom kontekstu, EDPB bi želio još jednom naglasiti da, kako bi izvršili svoje zadatke i ovlasti, nadzorna tijela moraju imati dovoljno ljudskih, tehničkih i financijskih resursa. Prema tome, nažalost nema informacija o imenovanim nadzornim tijela, posebice PIPC-u. EDPB stoga ponavlja svoj zahtjev Europskoj komisiji za davanje dodatnih informacija o tom pitanju.

181. U konačnici, EDPB bi želio istaknuti da gotovo nema izjava, primjera ili brojki u nacrtu odluke koji se odnose na nadzorne aktivnosti kao i na pravnu provedbu zakona o zaštiti podataka od strane nadzornih tijela u području izvršavanja zakonodavstva i nacionalne sigurnosti. To bi bilo korisno u kontekstu procjene učinkovitosti nadzornih tijela.

1.8. Pravni lijek i sudska zaštita

182. EDPB podsjeća da je za primjerenu razinu zaštite podataka važno da ispitanici imaju sveobuhvatne pravne lijekove i sudsku zaštitu od neovlaštenog pristupa ili obrade podataka. Ti pravni lijekovi moraju biti dovoljni kako bi se ispitaniku omogućilo dobivanje pristupa podatcima pohranjenima o njemu i zahtijevanja ispravka ili brisanja istih.

183. Uzimajući u obzir presude *Schrems I* i *Schrems II* Suda Europske unije, jasno je da je, uz pravo obraćanja nadležnim tijelima, od izuzetne važnosti i djelotvorna sudska zaštita u značenju članka 47. stavka 1. Povelje radi pretpostavke primjerenosti prava treće zemlje.

184. EDPB prepoznaje da je Koreja uspostavila različite načine izvršavanja prava pojedinaca na pristup, zadržavanje, brisanje i obustavu prema PIPA-i. Ta se prava mogu izvršiti preko samog voditelja obrade ili putem žalbe koja se podnosi PIPC-u ili drugom nadzornom tijelu, npr. Nacionalnoj komisiji za ljudska prava. Nadalje, EDPB prepoznaje mogućnost osporavanja odluke voditelja obrade ili javnih tijela kao odgovor na njihov zahtjev na temelju Zakona o upravnim sporovima.

185. Dodatno, EDPB razumije iz objašnjenja koje je dala Europska komisija da pojedinci mogu osporiti radnje tijela za izvršavanja zakonodavstva i nacionalnu sigurnost pred nadležnim sudovima prema Zakonu o upravnim sporovima i Zakonu o Ustavnom sudu te da imaju mogućnost dobivanja naknade za štetu na temelju Državnog zakona o naknadama[92].

186. Međutim, u ovom kontekstu je EDPB zabrinut o učinkovitoj sudskoj zaštiti za pojedince iz EU-a u slučajevima nacionalne sigurnosti ako nije uključen nijedan državljanin Koreje. Kako je navedeno u odjeljku 33. i dalje, tijela nacionalne sigurnosti nisu obvezne obavijestiti ispitanike o prikupljanju i obradi njihovih osobnih podataka. S obzirom na to da je mnogo teže dobiti djelotvornu pravnu zaštitu u takvim slučajevima, EDPB bi želio naglasiti da su ovdje potrebne određene pravne zaštitne mjere ako su uključeni podatci preneseni iz EGP-a. Te zaštitne mjere moraju ispitanicima omogućiti poduzimanje učinkovitih radnji protiv nezakonite obrade podataka na pravno siguran način bez prepreka pretjerano suženih postupovnih zahtjeva, primjerice nametanjem tereta dokazivanja koje ne mogu ispuniti bez znanja o obradi. Nadalje, ispitanici se moraju moći obratiti nadležnom tijelu koje udovoljava zahtjevima članka 47. Povelje Europske unije o temeljnim pravima, tj. koje je nadležno za određivanja da se odvija obrada osobnih podataka, za potvrdu zakonitosti obrade te koje ima izvršne ovlasti za primjenu pravnog lijeka u slučaju nezakonite obrade osobnih podataka. Prema tome, samo pravo na žalbu, primjerice NHRC-u, ne bi bilo dovoljno. Stoga EDPB poziva Komisiju na detaljnije objašnjenje

[92] Vidjeti Prilog II., 3.2.4. u vezi s 2.4.3.

načina na koji se ovi zahtjevi primjenjuju u postupovnom i materijalnom smislu, primjerice je li ispitanicima moguće obratiti se PIPC-u i sudu bez potrebe za dokazivanjem dotične obrade podataka.

187. Dodatno, EDPB je uočio da nacrt odluke predviđa mehanizam upućivanja žalbi, odnosno da pojedinci iz EU-a mogu podnijeti žalbu PIPC-u putem nacionalnog nadležnog tijela za zaštitu podataka ili EDPB-a. PIPC će tada obavijestiti pojedinca putem istog kanala kad je istraga zaključena[93]. EDPB pozdravlja napore pojednostavljivanja pristupa sudskoj zaštiti u odnosu na korejska tijela nacionalne sigurnosti. Istodobno, EDPB se zalaže za to da se takav mehanizam upućivanja usmjerava preko europskih nacionalnih tijela za zaštitu podataka, a ne preko EDPB-a jer su nadležni i bliži rješavaju žalbi pojedinaca.

188. Nadalje, EDPB ističe moguću proturječnost za dobrovoljna objavljivanja. S jedne strane, nacrt odluke navodi da pojedinci mogu zatražiti sudsku zaštitu ako su njihovi podatci nezakonito otkriveni na temelju zahtjeva za dobrovoljno objavljivanje, među ostalim protiv tijela za izvršavanje zakonodavstva koje je izdalo zahtjev[94]. S druge strane, u nacrtu odluke poziva se na zahtjev izravnog učinka u odnosu na prava pojedinca na osporavanje radnji javnih tijela navodeći (isključivo) obvezujuće zahtjeve za objavljivanje kao primjer slučaja ako se smatra da administrativna radnja izravno utječe na pravo na privatnost[95]. EDPB iz objašnjenja Europske komisije shvaća da zapravo nema ograničenja mogućnosti sudske zaštite od zahtjeva za dobrovoljno otkrivanje te stoga poziva Europsku komisiju na dodatno pojašnjenje toga u odluci, u području izvršavanja zakonodavstva i u području nacionalne sigurnosti (za razliku od odjeljka o provedbi zakona, odjeljak o dobrovoljnim objavljivanjima radi nacionalne sigurnosti ne sadržava izričite izjave o sudskoj zaštiti u ovom kontekstu).

[93] Vidjeti uvodnu izjavu 205. i Prilog I., str. 19. nacrta odluke.
[94] Vidjeti uvodnu izjavu 166. nacrta odluke.
[95] Vidjeti uvodnu izjavu 181. (izvršavanje zakonodavstva) i uvodne izjave 208. i 181. (nacionalna sigurnost) nacrta odluke.