Stanovisko 32/2021 týkajúce sa návrhu vykonávacieho rozhodnutia Európskej komisie podľa nariadenia (EÚ) 2016/679 o primeranej ochrane osobných údajov v Kórejskej republike

Verzia 1.0

Prijaté 24. septembra 2021

OBSAH

so zreteľom na článok 70 ods. 1 písm. s) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „**všeobecné nariadenie o ochrane údajov**“),

so zreteľom na Dohodu o Európskom hospodárskom priestore (ďalej len „**EHP**“), najmä na prílohu XI a protokol 37 k uvedenej dohode, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018[1],

so zreteľom na články 12 a 22 svojho rokovacieho poriadku,

PRIJAL TOTO STANOVISKO:

1. ZHRNUTIE

1. Európska komisia začala 16. júna 2021 formálny postup, ktorého cieľom je prijať návrh vykonávacieho rozhodnutia (ďalej len „**návrh rozhodnutia**“) o primeranej ochrane osobných údajov v Kórejskej republike podľa zákona o ochrane osobných informácií v súlade so všeobecným nariadením o ochrane údajov[2].

2. V ten istý deň Európska komisia požiadala o stanovisko Európsky výbor pre ochranu údajov (ďalej len „**EDPB**“)[3]. EDPB vypracoval posúdenie primeranosti úrovne ochrany poskytovanej v Kórejskej republike na základe preskúmania samotného návrhu rozhodnutia, ako aj na základe analýzy dokumentácie, ktorú sprístupnila[4] Európska komisia.

3. EDPB sa zameral na posúdenie všeobecných aspektov všeobecného nariadenia o ochrane údajov, pokiaľ ide o návrh rozhodnutia, ako aj prístupu orgánov verejnej moci k osobným údajom prenášaným z EHP na účely presadzovania práva a národnej bezpečnosti vrátane právnych prostriedkov nápravy dostupných pre jednotlivcov v EHP. EDPB takisto posúdil, či sú záruky poskytované podľa kórejského právneho rámca zavedené a účinné.

4. EDPB použil ako hlavný referenčný materiál pre tento dokument svoje referenčné kritérium primeranosti podľa všeobecného nariadenia o ochrane údajov[5] (ďalej len „**referenčné kritérium primeranosti podľa všeobecného nariadenia o ochrane údajov**“) prijaté vo februári 2018 a odporúčania EPDB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania[6].

[1] Odkazy na „**členské štáty**“ uvedené v tomto stanovisku by sa mali chápať ako odkazy na „členské štáty EHP“.
[2] Pozri tlačovú správu https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Tamže.
[4] EPDB pri svojej analýze vychádzal z úradných prekladov, ktoré pripravila kórejská vláda.
[5] WP254, referenčné kritérium primeranosti podľa všeobecného nariadenia o ochrane údajov, 6. februára 2018 (schválené EDPB, pozri https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Pozri odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania, prijaté 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Oblasti konvergencie

5. Hlavným cieľom EDPB je predložiť Európskej komisii stanovisko týkajúce sa primeranosti úrovne ochrany poskytovanej jednotlivcom, ktorých osobné údaje sa prenášajú do Kórejskej republiky. Treba si uvedomiť, že EDPB neočakáva, že kórejský rámec ochrany údajov bude kopírovať európske právne predpisy o ochrane údajov.

6. Pripomína však, že na to, aby bol považovaný za právny rámec, ktorý poskytuje primeranú úroveň ochrany, sa v článku 45 všeobecného nariadenia o ochrane údajov a judikatúre Súdneho dvora Európskej únie (ďalej len „**SDEÚ**“) vyžaduje, aby právne predpisy tretej krajiny boli v súlade s podstatou základných zásad zakotvených vo všeobecnom nariadení o ochrane údajov. Kórejský rámec ochrany údajov v tejto súvislosti obsahuje viacero prvkov, ktoré sa podobajú prvkom európskeho rámca ochrany údajov, konkrétne obidva majú jeden hlavný právny predpis, ktorý sa vzťahuje na verejný aj súkromný sektor a ktorý dopĺňajú sektorové legislatívne akty.

7. Pokiaľ ide o obsah, EDPB poukazuje na kľúčové oblasti súladu medzi rámcom všeobecného nariadenia o ochrane údajov a kórejským rámcom ochrany údajov v prípade určitých základných ustanovení, ako sú napríklad pojmy (napr. „osobné informácie“, „spracúvanie“, „dotknutá osoba“); dôvody zákonného a spravodlivého spracúvania na legitímne účely; obmedzenie účelu; kvalita údajov a proporcionalita; uchovávanie, bezpečnosť a dôvernosť údajov; transparentnosť; a osobitné kategórie údajov.

8. Okrem uvedených informácií EDPB víta úsilie, ktoré vyvinula Európska komisia a kórejské orgány, aby zaistili, že Kórejská republika poskytuje úroveň ochrany primeranú úrovni ochrany, ktorá sa zaručuje všeobecným nariadením o ochrane údajov, prostredníctvom prijatia systému oznámení kórejským dozorným orgánom (netýka sa to len osobných údajov prenášaných z EHP do Kórey) s cieľom preklenúť rozdiely medzi všeobecným nariadením o ochrane údajov a kórejským rámcom ochrany údajov. EDPB by v tejto súvislosti chcel zdôrazniť význam týchto oznámení pre posúdenie primeranosti ochrany osobných údajov v Kórejskej republike, pričom napríklad uvádza, že oznámenia poskytujú relevantné objasnenia niektorých dôležitých záruk, a to aj v súvislosti s rozsahom uplatňovania výnimiek zo zákona o ochrane osobných informácií na spracúvanie pseudonymizovaných osobných informácií na vedecké, výskumné a štatistické účely, na následné prenosy a pravidlá, ktoré sa uplatňujú v súvislosti s prístupom orgánov verejnej moci k údajom.

1.2. Výzvy

9. Hoci EDPB stanovil, že mnohé aspekty kórejského rámca ochrany údajov sú v podstate rovnocenné aspektom európskeho rámca ochrany údajov, zároveň dospel k záveru, že jestvujú určité aspekty, ktoré si môžu vyžadovať podrobnejšie preskúmanie a objasnenie. Konkrétne sa EDPB domnieva, že treba ďalej posúdiť tieto body, aby sa zabezpečilo dosiahnutie v podstate rovnocennej úrovne ochrany. Európska komisia by zároveň mala tieto body dôkladne monitorovať.

1.2.1. Všeobecné aspekty

10. EDPB berie na vedomie, že oznámenie č. 2021-1 *má význam správneho pravidla a je pre prevádzkovateľa osobných informácií právne záväzné v tom zmysle, že každé porušenie tohto oznámenia možno považovať za porušenie príslušných ustanovení zákona o ochrane osobných informácií*[7]. No vzhľadom na to, že oznámenie samo osebe neobsahuje dodatočné pravidlá, ale skôr objasnenie toho, ako by sa malo znenie zákona o ochrane osobných informácií chápať pri uplatňovaní, a vzhľadom na jeho celkový význam, najmä pokiaľ ide o ustanovenia o pseudonymizácii v rámci zákona o ochrane osobných informácií, ktoré sú podľa chápania EDPB predmetom prebiehajúcich súdnych konaní, EDPB vyzýva Európsku komisiu, aby poskytla ďalšie informácie o záväznej povahe, vykonateľnosti a platnosti oznámenia č. 2021-1, a odporučil by dôkladné monitorovanie dodržiavania

[7] Pozri oddiel I prílohy I k návrhu rozhodnutia.

tohto oznámenia v praxi, najmä v súvislosti s jeho uplatňovaním nielen kórejským dozorným orgánom, ale aj súdmi, obzvlášť ak rovnocenná úroveň ochrany, ktorú poskytuje kórejský právny rámec, vychádza z objasnení, ktoré sú v ňom stanovené.

1.2.2. Všeobecné aspekty ochrany údajov

11. EDPB v súvislosti s rozsahom uplatňovania rozhodnutia o primeranosti konštatuje, že sa bude vzťahovať na prenosy z právneho rámca EHP verejným aj súkromným „prevádzkovateľom osobných informácií“, ktorí patria do rozsahu pôsobnosti zákona o ochrane osobných informácií. EDPB chápe, že do tohto pojmu sú zahrnuté subjekty pôsobiace ako sprostredkovatelia v zmysle GDPR, v záujme predísť nedorozumeniam však vyzýva Európsku komisiu, aby lepšie objasnila, že rozhodnutie o primeranosti sa bude vzťahovať aj na prenosy „sprostredkovateľom“ v Kórei.

12. Dôležitý aspekt, na ktorý by chcel EDPB upozorniť, sa týka pojmu „pseudonymizované informácie“ v kórejskom rámci ochrany údajov. Podľa kórejskej právnej úpravy sa na spracúvanie pseudonymizovaných osobných informácií vzťahujú výnimky z viacerých príslušných ustanovení vrátane ustanovení o individuálnych právach dotknutých osôb a uchovávaní údajov. Podľa Európskej komisie sa to týka len prípadov, keď sa pseudonymizované osobné informácie spracúvajú na účely štatistiky, vedeckého výskumu či archivácie vo verejnom záujme. Toto tvrdenie však predovšetkým vychádza z oznámenia č. 2021-1, z čoho vyplýva, že uvedená potreba dodatočných informácií o záväznej povahe, vykonateľnosti a platnosti tohto oznámenia, ako aj ich monitorovanie má v tejto súvislosti značný význam. EDPB navyše vyzýva Európsku komisiu, aby ďalej posúdila dôsledky pseudonymizácie podľa kórejského práva a predovšetkým spôsob, akým to môže ovplyvniť základné práva a slobody dotknutých osôb, ktorých osobné údaje sa na základe rozhodnutia o primeranosti prenášajú do Kórejskej republiky. EDPB vyzýva Európsku komisiu, aby najmä ďalej posúdila odchýlky uvedené v článku 28-7 zákona o ochrane osobných informácií a článku 40 ods. 3 zákona o používaní a ochrane úverových informácií a aby dôkladne monitorovala ich uplatňovanie a príslušnú judikatúru s cieľom zabezpečiť, že pri spracúvaní osobných údajov prenášaných na základe rozhodnutia o primeranosti na tieto účely sa práva dotknutých osôb neprimerane neobmedzujú.

13. EDPB ďalej konštatuje, že právo odvolať súhlas sa v kórejskej právnej úprave vyskytuje iba za osobitných podmienok, a preto vyzýva Európsku komisiu, aby ďalej posúdila dôsledky neexistencie všeobecného práva odvolať súhlas a poskytla ďalšie záruky, a tak zabezpečila nevyhnutnú úroveň ochrany údajov za každých okolností, prípadne aj objasnením úlohy práva na pozastavenie spracúvania na základe zákona o ochrane osobných informácií, ak všeobecné právo odvolať súhlas neexistuje.

14. Pokiaľ ide o následné prenosy, EDPB uznáva, že informovaný súhlas dotknutej osoby sa vo všeobecnosti použije ako základ pre prenosy údajov od prevádzkovateľa osobných informácií so sídlom v Kórei príjemcovi so sídlom v tretej krajine a že oznámenie č. 2021-1 počíta s tým, že jednotlivci musia byť informovaní o tretej krajine, do ktorej sa ich údaje poskytnú. EDPB však vyzýva Európsku komisiu, aby zabezpečila, že informácie, ktoré sa majú poskytnúť dotknutej osobe, zahŕňajú aj informácie o rizikách, ktoré prenosy môžu predstavovať z dôvodu absencie primeranej ochrany v tretej krajine, ako aj absencie primeraných záruk. EDPB by okrem toho uvítal, ak by rozhodnutie o primeranosti obsahovalo uistenia, že kórejskí prevádzkovatelia osobných informácií neprenesú osobné údaje do tretej krajiny za žiadnych okolností, keď by nebolo možné poskytnúť platný súhlas podľa všeobecného nariadenia o ochrane údajov, napríklad v dôsledku nerovnováhy postavenia.

15. Čo sa týka vymenovania členov kórejského dozorného orgánu, hoci by formálny postup bol v súlade so všeobecným nariadením o ochrane údajov, a teda by prešiel testom rovnocennosti [test of equivalence] s právnym rámcom EHP, EDPB by chcel vyzvať Európsku komisiu, aby monitorovala akýkoľvek vývoj, ktorý by mohol ovplyvniť nezávislosť členov dozorného orgánu Južnej Kórey.

16. Pokiaľ ide o rozpočet, pričom sa opäť vychádza z informácií poskytnutých Európskou komisiou, neuvádzajú sa žiadne osobitosti personálu Komisie pre ochranu osobných informácií [Personal Information Protection Commission] ani finančné zdroje, ktoré má k dispozícii. EDPB by preto v súvislosti s týmito dvomi relevantnými témami uvítal zahrnutie dodatočných informácií do návrhu rozhodnutia.

1.2.3. O prístupe orgánov verejnej moci k údajom prenášaným do Kórejskej republiky

17. EDPB zanalyzoval kórejský právny rámec aj vzhľadom na prístup vlády k osobným údajom prenášaným z EHP do Kórey na účely presadzovania práva a národnej bezpečnosti. Hoci EDPB uznáva vyhlásenia a záruky, ktoré poskytla kórejská vláda, uvedené v prílohe II k návrhu nariadenia, identifikoval niekoľko aspektov, ktoré si vyžadujú objasnenie alebo vzbudzujú obavy.

18. EDPB konštatuje, že ustanovenia zákona o ochrane osobných informácií sa bez obmedzenia uplatňujú v oblasti presadzovania práva. EDPB takisto poznamenáva, že spracúvanie údajov v oblasti národnej bezpečnosti podlieha obmedzenejšiemu súboru ustanovení zakotvených v zákone o ochrane osobných informácií.

19. Pokiaľ ide o dobrovoľné sprístupnenie osobných informácií poskytovateľmi telekomunikačných služieb národným bezpečnostným orgánom, EDPB vyjadruje znepokojenie nad tým, že vzťah medzi oddielom 3 prílohy I k návrhu rozhodnutia, v ktorom sa stanovuje, že ak poskytovatelia dobrovoľne vyhovejú žiadosti, musia o tom v zásade informovať dotknutú osobu, a článkom 58 ods. 1 pododsekom 2 zákona o ochrane osobných informácií, t. j. čiastočnou výnimkou na účely národnej bezpečnosti, je nejasný. Mohlo by to zapríčiniť, že požiadavky na informácie nebudú účinné, čo by znamenalo, že pre dotknuté osoby by bolo oveľa náročnejšie uplatniť si práva na ochranu údajov, najmä právo na súdny prostriedok nápravy.

20. Hoci sa to v návrhu rozhodnutia výslovne neuvádza, EDPB podľa vysvetlení poskytnutých Európskou komisiou chápe, že kórejský právny rámec neumožňuje hromadné zachytávanie údajov o telekomunikácii. Z toho dôvodu by nedávna judikatúra Európskeho súdu pre ľudské práva (ďalej „ESĽP“) týkajúca sa režimov hromadného zachytávania nebola priamo príslušná pre posúdenie úrovne ochrany údajov v Kórei.

21. Návrh rozhodnutia neobsahuje žiadne informácie o právnom rámci pre následné prenosy v oblasti národnej bezpečnosti. Hoci EDPB chápe, že podľa Európskej komisie sú následné prenosy na účely národnej bezpečnosti upravené všeobecnými zárukami a zásadami podľa ústavného rámca a zákona o ochrane osobných informácií v dostatočnej miere, vyjadruje znepokojenie, či takúto úpravu možno považovať za splnenie požiadaviek na presnosť a jasnosť práva a či sa v nej zakotvujú účinné a vymožiteľné záruky. Záruky, na ktoré Európska komisia odkazuje, sú prevažne všeobecnej povahy a pri riešení osobitných okolností a podmienok, za ktorých sa môžu uskutočniť následné prenosy na účely národnej bezpečnosti, nevychádzajú z právneho základu. V tejto súvislosti EDPB takisto konštatuje, že Európska komisia nezohľadnila, či sú medzi Kórejskou republikou a tretími krajinami alebo medzinárodnými organizáciami uzavreté medzinárodné dohody, ktoré môžu obsahovať osobitné ustanovenia týkajúce sa medzinárodného prenosu osobných údajov orgánmi presadzovania práva a/alebo spravodajskými službami do tretích krajín. EDPB sa domnieva, že uzavretie dvojstranných a viacstranných dohôd s tretími krajinami na účely presadzovania práva alebo spravodajskej spolupráce s pravdepodobnosťou môže ovplyvniť posudzovanie kórejského právneho rámca ochrany údajov.

22. EDPB konštatuje, že dozor nad orgánmi presadzovania práva v trestných veciach, ako aj národnými bezpečnostnými orgánmi zabezpečuje kombinácia rôznych vnútorných a vonkajších orgánov, konkrétne Komisia pre ochranu osobných informácií, ktorej boli zverené dostatočné výkonné právomoci.

23. Účinné prostriedky nápravy si vyžadujú, aby sa dotknuté osoby mohli obrátiť na príslušný orgán, ktorý spĺňa požiadavky článku 47 Charty základných práv Európskej únie (ďalej len „**Charta**“), t. j. orgán, ktorý má právomoc určiť, či sa údaje spracúvajú, overiť zákonnosť spracúvania a ktorý má vymožiteľné nápravné právomoci v prípade, že je spracúvanie údajov nezákonné. Na základe uvedených skutočností EDPB žiada Európsku komisiu, aby objasnila, či sťažnosť predložená Komisii pre ochranu osobných informácií alebo akákoľvek žaloba na súde podlieha hmotnoprávnym a/alebo procedurálnym požiadavkám, ako je dôkazné bremeno, a či by jednotlivci v EHP dokázali splniť takúto požiadavku.

1.3. Záver

24. EDPB sa domnieva, že toto rozhodnutie o primeranosti má zásadný význam aj vzhľadom na to – s výnimkami uvedenými v stanovisku –, že sa bude vzťahovať na prenosy vo verejnom aj v súkromnom sektore.

25. EDPB víta úsilie Európskej komisie a kórejských orgánov o zosúladenie kórejského právneho rámca s európskym. Zlepšenia, ktoré má priniesť oznámenie č. 2021-1 na preklenutie niektorých rozdielov medzi týmito dvoma rámcami, sú veľmi dôležité a dobre prijaté. EDPB však konštatuje, že naďalej existuje niekoľko znepokojujúcich skutočností, a to aj pokiaľ ide o oznámenie č. 2021-1, a zároveň potreba ďalšieho objasnenia niektorých problémov. Európskej komisii odporúča, aby sa zamerala na tieto znepokojujúce skutočnosti a žiadosti o objasnenie, ktoré uvádza EDPB, a poskytla ďalšie informácie a vysvetlenia v súvislosti s problémami predloženými v tomto stanovisku.

2. ÚVOD

2.1. Kórejský rámec ochrany údajov

26. Hlavný právny predpis, ktorým sa upravuje ochrana údajov v Kórejskej republike, je zákon o ochrane osobných informácií [Personal Information Protection Act] (zákon č. 10465 z 29. marca 2011, naposledy zmenený zákonom č. 16930 zo 4. februára 2020). Dopĺňa ho vykonávací dekrét (prezidentský dekrét č. 23169 z 29. septembra 2011, naposledy zmenený prezidentským dekrétom č. 30892 zo 4. augusta 2020, ďalej len „**vykonávací dekrét k zákonu o ochrane osobných informácií**“), ktorý je právne záväzný a vymožiteľný.

27. Do kórejského rámca ochrany údajov okrem zákona o ochrane osobných informácií patria regulačné „oznámenia“, ktoré vydáva kórejský dozorný orgán – Komisia pre ochranu osobných informácií a v ktorých sa stanovujú ďalšie pravidlá týkajúce sa výkladu a uplatňovania zákona o ochrane osobných informácií. Komisia pre ochranu osobných informácií nedávno prijala oznámenie č. 2021-1 z 21. januára 2021 (ktorým sa zmenilo prechádzajúce oznámenie č. 2020-10 z 1. septembra 2020, ďalej len „**oznámenie č. 2021-1**“) o výklade, uplatňovaní a presadzovaní určitých ustanovení zákona o ochrane osobných informácií. Konkrétnejšie toto oznámenie je výsledkom diskusií o primeranosti, ktoré sa uskutočnili medzi kórejskými orgánmi a Európskou komisiou. Zahŕňa objasnenia zamerané na uplatňovanie osobitných ustanovení zákona o ochrane osobných informácií vrátane ustanovení týkajúcich sa spracúvania osobných údajov prenášaných do Kórey na základe predpokladaného rozhodnutia o primeranosti[8] a *má význam správneho pravidla a je pre prevádzkovateľa osobných informácií právne záväzné v tom zmysle, že každé porušenie tohto oznámenia možno považovať za porušenie príslušných ustanovení zákona o ochrane osobných informácií*[9]. EDPB by v tejto súvislosti chcel poznamenať, že napriek tomu, že sa v návrhu rozhodnutia odkazuje na oznámenie ako na „doplnkové pravidlá“ [supplementary rules], toto oznámenie neobsahuje dodatočné pravidlá ako

[8] Pozri oddiel I prílohy I k návrhu rozhodnutia.
[9] Tamže.

také, ale skôr vysvetlenia zamerané na objasnenie toho, ako by sa malo znenie zákona o ochrane osobných informácií chápať pri uplatňovaní, najmä pokiaľ ide o údaje prenášané z EHP. EDPB by v tomto kontexte odporučil dôkladné monitorovanie dodržiavania oznámenia č. 2021-1 v praxi, najmä pokiaľ ide o jeho uplatňovanie nielen Komisiou pre ochranu osobných informácií, ale aj súdmi, obzvlášť ak je rovnocenná úroveň ochrany poskytovaná kórejským právnym rámcom založená na objasneniach uvedených v oznámení č. 2021-1.

28. V ďalších relevantných právnych predpisoch o ochrane údajov patriacich do kórejského legislatívneho rámca sa stanovujú pravidlá spracúvania osobných údajov v konkrétnych odvetviach, napr.:

    - zákon o používaní a ochrane úverových informácií vrátane vykonávacieho dekrétu k nemu (ďalej len „**vykonávací dekrét k zákonu o používaní a ochrane úverových informácií**“), v ktorom sa stanovujú osobitné pravidlá príslušné pre komerčných prevádzkovateľov a špecializované subjekty (ako sú ratingové agentúry, finančné inštitúcie) pri spracúvaní osobných úverových informácií, ktoré sú potrebné na určenie úverovej bonity strán finančnej alebo obchodnej transakcie,

    - zákon o podpore využívania informačnej a komunikačnej siete a ochrane údajov, a

    - zákon o ochrane súkromia komunikácie.

29. Pokiaľ ide o prístup vlády [government access], EDPB okrem príslušných ustanovení zákona o ochrane osobných informácií a zákona o ochrane súkromia komunikácie zohľadnil niekoľko ďalších právnych predpisov, t. j. zákon o trestnom konaní, zákon o telekomunikáciách, zákon o oznamovaní a používaní špecifikovaných informácií o finančných transakciách a zákon o Národnej spravodajskej službe.

2.2. Rozsah posúdenia EDPB

30. Návrh rozhodnutia Európskej komisie je výsledkom posúdenia kórejského rámca ochrany údajov a následných diskusií s kórejskou vládou. V súlade s článkom 70 ods. 1 písm. s) všeobecného nariadenia o ochrane údajov sa od EDPB očakáva, že poskytne nezávislé stanovisko k zisteniam Európskej komisie, určí prípadné nedostatky v rámci primeranosti a bude sa usilovať o vypracovanie návrhov na ich riešenie.

31. S cieľom predísť opakovaniu a pomôcť pri posudzovaní kórejského právneho rámca sa EDPB rozhodol zamerať na niektoré konkrétne body uvedené v návrhu rozhodnutia a poskytnúť svoju analýzu a stanovisko k týmto bodom, pričom upúšťa od opakovania väčšiny skutkových zistení a posúdení v prípadoch, keď EDPB nemá žiadny dôvod domnievať sa, že právo Kórejskej republiky nie je v podstate rovnocenné s právom v EHP. Veľmi dôležitá časť analýzy sa v súlade s judikatúrou SDEÚ navyše týka právneho režimu prístupu národných bezpečnostných orgánov k osobným údajom prenášaným do Kórejskej republiky a postupov kórejských národných bezpečnostných orgánov.

32. EDPB vo svojom posúdení zohľadnil platný európsky rámec ochrany údajov vrátane článkov 7, 8 a 47 Charty, ktorými sa chráni právo na súkromný a rodinný život, právo na ochranu osobných údajov a právo na účinný prostriedok nápravy a spravodlivý proces, a článku 8 Európskeho dohovoru o ľudských právach, ktorým sa chráni právo na súkromný a rodinný život. Okrem uvedených ustanovení EDPB zohľadnil aj požiadavky všeobecného nariadenia o ochrane údajov a relevantnú judikatúru.

33. Cieľom tohto dokumentu je poskytnúť Európskej komisii stanovisko k posúdeniu primeranosti úrovne ochrany v Kórejskej republike. Pojem „primeraná úroveň ochrany“, ktorý existoval už podľa smernice 95/46, SDEÚ ďalej rozvinul. Je dôležité pripomenúť si normu stanovenú SDEÚ v rozsudku vo veci Schrems I, a to že – zatiaľ čo „úroveň ochrany“ v tretej krajine musí byť „v podstate rovnocenná“ úrovni ochrany zaručenej v EÚ – „*prostriedky, ktoré v tomto ohľade použije táto tretia krajina na*

zabezpečenie takejto úrovne ochrany, môžu byť rozdielne od tých, ktoré sa zaviedli v rámci EÚ“[10]. Cieľom preto nie je odzrkadľovať každý jeden bod európskych právnych predpisov, ale stanoviť základné prvky a hlavné požiadavky preskúmavaných právnych predpisov. Primeranosť možno dosiahnuť kombináciou práv dotknutých osôb a povinností tých, ktorí spracúvajú osobné údaje alebo vykonávajú kontrolu nad takýmto spracúvaním, a dozoru zo strany nezávislých orgánov. Pravidlá ochrany údajov sú však účinné len vtedy, ak sú vymožiteľné a v praxi sa dodržiavajú. Preto je potrebné zvážiť nielen obsah pravidiel týkajúcich sa osobných údajov prenášaných do tretej krajiny alebo medzinárodnej organizácii, ale aj systém zavedený na zabezpečenie účinnosti takýchto pravidiel. Efektívne mechanizmy presadzovania sú mimoriadne dôležité pre účinnosť pravidiel ochrany údajov[11].

2.3. Všeobecné pripomienky a obavy

2.3.1. Medzinárodné záväzky prijaté Kórejskou republikou

34. Podľa článku 45 ods. 2 písm. c) všeobecného nariadenia o ochrane údajov a referenčného kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov,[12] Európska komisia pri posudzovaní primeranosti úrovne ochrany v tretej krajine zohľadňuje aj medzinárodné záväzky, ktoré dotknutá krajina prevzala, alebo iné záväzky vyplývajúce z účasti tretej krajiny na viacstranných alebo regionálnych systémoch, najmä vo vzťahu k ochrane osobných údajov, ako aj plnenie takýchto záväzkov.

35. Kórea je zmluvnou stranou niekoľkých medzinárodných dohôd, v ktorých sa zaručuje právo na súkromie. Ide o Medzinárodný pakt o občianskych a politických právach (článok 17), Dohovor o právach osôb so zdravotným postihnutím (článok 22) a Dohovor o právach dieťaťa (článok 16). Popritom Kórea ako člen OECD dodržiava rámec OECD na ochranu súkromia, predovšetkým usmernenia k ochrane súkromia a cezhraničným tokom osobných údajov.

36. EDPB okrem toho berie na vedomie účasť Kórey ako pozorovateľského štátu na činnostiach poradného výboru Dohovoru Rady Európy 108(+), hoci sa ešte nerozhodla, či k dohovoru pristúpi.

2.3.2. Rozsah pôsobnosti rozhodnutia o primeranosti

37. Podľa odôvodnenia 5 návrhu rozhodnutia Európska komisia dospela k záveru, že Kórejská republika zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných od prevádzkovateľa alebo sprostredkovateľa v Únii prevádzkovateľom osobných informácií (napr. fyzickým alebo právnickým osobám, organizáciám, verejným inštitúciám), ktorí patria do rozsahu uplatňovania zákona o ochrane osobných informácií, s výnimkou spracúvania osobných údajov na účely vykonávania misijných činností náboženskými organizáciami a vymenovania kandidátov politickými stranami[13] alebo spracúvania osobných úverových informácií podľa zákona o používaní a ochrane úverových informácií prevádzkovateľmi, ktorí podliehajú dozoru Komisie pre finančné služby [Financial Services Commission].

38. EDPB konštatuje, že rozhodnutie o primeranosti sa bude vzťahovať na prenosy z právneho rámca EHP verejným aj súkromným „prevádzkovateľom osobných informácií“, ktorí patria do rozsahu pôsobnosti zákona o ochrane osobných informácií. EDPB chápe, že do pojmu „prevádzkovatelia osobných informácií“ sú zahrnuté aj subjekty pôsobiace ako sprostredkovatelia v zmysle všeobecného nariadenia o ochrane údajov, keďže zákon o ochrane osobných informácií sa na ne bude vzťahovať rovnakým spôsobom a keďže, ak prevádzkovateľ osobných informácií (ďalej len „zadávateľ“)

[10] Vec C-362/14, Maximillian Schrems/Data Protection Commissioner, 6. októbra 2015, ECLI:EU:C:2015:650, body 73 – 74.
[11] WP254, s. 2.
[12] WP254, s. 2.
[13] Viac informácií sa nachádza v oddiele 3.1.2 tohto stanoviska.

[outsourcer] zapojí do spracúvania osobných údajov tretiu stranu (ďalej len „externý poskytovateľ spracúvania“) [outsourcee], budú sa uplatňovať osobitné povinnosti. S cieľom predísť nedorozumeniam EDPB však vyzýva Európsku komisiu, aby objasnila, že rozhodnutie o primeranosti sa bude vzťahovať aj na prenosy „sprostredkovateľom“ v Kórei a že úroveň ochrany osobných údajov prenášaných z EHP nebude ohrozená ani v týchto prípadoch.

39. Okrem toho, ak sa prihliadne na to, že rozhodnutie o primeranosti sa vzťahuje aj na prenosy osobných údajov medzi orgánmi verejnej moci, EDPB chápe, že sa to bude vzťahovať aj na prenosy medzi dozornými orgánmi pre ochranu údajov, a v záujme jednoznačnosti vyzýva Európsku komisiu, aby sa touto otázkou osobitne zaoberala.

40. Ďalej, pokiaľ ide o subjekty vylúčené z rozsahu uplatňovania rozhodnutia o primeranosti, EDPB by chcel zdôrazniť, že pre rozhodnutie o primeranosti by bolo prínosné, ak by sa jasnejšie stanovili „obchodné organizácie“ podliehajúce dozoru Komisie pre ochranu osobných informácií (článok 45 ods. 3 zákona o používaní a ochrane úverových informácií), aby prevádzkovatelia a sprostredkovatelia so sídlom v EHP mohli jednoducho posúdiť, či dovozca takisto patrí do rozsahu uplatňovania rozhodnutia o primeranosti, pred tým, než prenesú údaje subjektom, ktoré patria do rozsahu uplatňovania zákona o používaní a ochrane úverových informácií, alebo prinajmenšom boli upozornení na potrebu posúdenia tohto aspektu.

41. EDPB v súvislosti s rozsahom pôsobnosti rozhodnutia o primeranosti podľa dodatočných vysvetlení Európskej komisie chápe, že ani Finančná spravodajská jednotka Kórey [Korea Financnial Intelligence Unit], ktorá je zriadená v rámci Komisie pre finančné služby a ktorá dohliada na predchádzanie praniu špinavých peňazí a financovaniu terorizmu v súlade so zákonom o oznamovaní a používaní špecifikovaných informácií o finančných transakciách[14], nepatrí do rozsahu pôsobnosti, keďže jej právomoc sa vzťahuje len na finančné inštitúcie, ktorých sa návrh rozhodnutia netýka. V článku 1 ods. 2 písm. c) návrhu rozhodnutia sa však z rozsahu pôsobnosti vylučujú len tí prevádzkovatelia osobných informácií, ktorí podliehajú dozoru Komisie pre finančné služby a ktorí spracúvajú osobné úverové informácie na základe zákona o používaní a ochrane úverových informácií. EDPB v tejto súvislosti vyzýva Európsku komisiu, aby objasnila, či sa na Finančnú spravodajskú jednotku Kórey a jej spracovateľské činnosti vzťahuje návrh rozhodnutia.

3. VŠEOBECNÉ ASPEKTY OCHRANY ÚDAJOV

3.1. Zásady týkajúce sa obsahu

42. Kapitola 3 referenčného kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov je venovaná zásadám týkajúcim sa obsahu. Systém tretej krajiny ich musí obsahovať, aby sa úroveň poskytovanej ochrany mohla považovať za takú, ktorá je v podstate rovnocenná s úrovňou ochrany zaručenou právnymi predpismi EÚ.

43. Hoci právo na ochranu osobných údajov nie je samo osebe výslovne zakotvené v kórejskej ústave, uznáva sa ako základné právo odvodené od ústavného práva na ľudskú dôstojnosť a usilovanie sa o šťastný život (článok 10), práva na súkromný život (článok 17) a práva na ochranu súkromia komunikácie (článok 18). Ako sa uvádza v návrhu rozhodnutia Európskej komisie[15], uznal to najvyšší súd aj ústavný súd. Toto uznanie EDPB berie na vedomie, keďže vyplýva z toho, že podľa článku 37 kórejskej ústavy ochrana údajov ako základné právo *„môže byť obmedzená len zákonom a vtedy, ak je*

[14] Pozri prílohu II, oddiel 2.2.3.1.
[15] Pozri odôvodnenie 8 návrhu rozhodnutia a príslušnú judikatúru uvedenú v poznámke pod čiarou č. 10 návrhu rozhodnutia. Zhrnutia rozhodnutí tejto judikatúry sú dostupné iba v angličtine.

to potrebné z dôvodu národnej bezpečnosti, udržania verejného poriadku alebo pre blaho verejnosti“ a že „*ani v prípade ich uloženia nemôžu tieto obmedzenia ovplyvňovať podstatu slobody alebo práva*“.

44. Európska komisia uviedla[16], že ústavný súd rozhodol, že aj cudzí štátni príslušníci sú držiteľmi základných práv. Pokiaľ ide o oficiálne vyhlásenia kórejskej vlády[17], hoci sa v judikatúre dosiaľ nerozhodovalo konkrétne o práve cudzích štátnych príslušníkov na súkromie, právni vedci vo všeobecnosti uznávajú, že v článkoch 12 – 22 ústavy sa stanovujú „práva ľudských bytostí“. Kórejská republika okrem toho prijala súbor zákonov v oblasti ochrany údajov, ktorými sa poskytujú záruky všetkým osobám bez ohľadu na ich štátnu príslušnosť, medzi ktoré sa zaraďuje aj zákon o ochrane osobných informácií. V tejto súvislosti EDPB berie na vedomie, že v článku 6 ods. 2 ústavy sa stanovuje, že postavenie cudzích štátnych príslušníkov je zaručené v súlade s medzinárodným právom a zmluvami, a judikatúrou uvedenou v návrhu rozhodnutia, podľa ktorej môže byť „cudzinec“ držiteľom „základných práv“. Vzhľadom na význam priznania práva na ochranu údajov „cudzím štátnym príslušníkom“, EDPB upriamuje pozornosť Európskej komisie na potrebu ďalej monitorovať judikatúru týkajúcu sa ochrany údajov ako základného práva priznaného nielen kórejským občanom, ale všetkým dotknutým osobám, čím sa zaistí, že úroveň ochrany fyzických osôb zaručená všeobecným nariadením o ochrane údajov nebude ohrozená pri prenose osobných údajov do Kórey na základe rozhodnutia o primeranosti.

3.1.1. Pojmy

45. Podľa referenčného kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov by sa v právnom rámci tretej krajiny mali nachádzať základné pojmy a/alebo zásady ochrany údajov. Aj keď tieto pojmy či zásady nemusia odzrkadľovať terminológiu použitú vo všeobecnom nariadení o ochrane údajov, mali by odrážať pojmy zakotvené v európskych právnych predpisoch o ochrane údajov a byť v súlade s nimi. Napríklad všeobecné nariadenie o ochrane údajov obsahuje tieto dôležité pojmy: „osobné údaje“, „spracúvanie osobných údajov“, „prevádzkovateľ“, „sprostredkovateľ“, „príjemca“, „citlivé údaje“[18].

46. Zákon o ochrane osobných informácií obsahuje niekoľko vymedzených pojmov, napríklad „osobné informácie“, „spracúvanie“ a „dotknutá osoba“, ktoré sa značne podobajú zodpovedajúcim pojmom vo všeobecnom nariadení o ochrane údajov.

3.1.1.1. Pojem „pseudonymizované údaje“

47. Spomedzi pojmov, ktoré sú vymedzené v zákone o ochrane osobných informácií, sa v článku 2 ods. 1 konkrétne vymedzujú osobné informácie ako akákoľvek z týchto informácií týkajúcich sa živej osoby: a) informácia obsahujúca celé meno, evidenčné číslo obyvateľa, vyobrazenie atď. konkrétnej osoby, vďaka čomu ju možno identifikovať; a b) informácia, na základe ktorej sa síce neidentifikuje konkrétna osoba, ale možno ju jednoducho skombinovať s inou informáciou, a tak identifikovať konkrétnu osobu. V prípade druhého typu informácie sa jednoduchosť skombinovania určuje primeraným prihliadnutím na čas, náklady, technológie atď., ktoré sú potrebné na identifikáciu osoby, ako je napríklad pravdepodobnosť získania iných informácií.

48. Navyše podľa článku 2 ods. 1 písm. c) zákona o ochrane osobných informácií sa „pseudonymizované informácie“ takisto považujú za osobné informácie. Pseudonymizované informácie sú vymedzené ako uvedené informácie podľa písm. a) alebo b), ktoré sú pseudonymizované v súlade s pododsekom 1-2, a teda na základe nich nemožno identifikovať konkrétnu osobu bez použitia alebo skombinovania informácií na obnovu ich pôvodného stavu. Informácie, ktoré sú plne anonymizované, nepatria do rozsahu uplatňovania zákona o ochrane osobných informácií. Podľa článku 58-2 zákona o ochrane

[16] Pozri odôvodnenie 9 návrhu rozhodnutia.
[17] Oddiel 1.1 prílohy II k návrhu rozhodnutia.
[18] WP254, s. 4.

osobných informácií sa zákon nevzťahuje na informácie, na základe ktorých nie je možné po ich skombinovaní s inými informáciami identifikovať konkrétnu osobu, pričom sa primerane prihliadne na čas, náklady, technológie atď.

49. Európska komisia v odôvodnení 17 svojho návrhu rozhodnutia uvádza, že toto zodpovedá vecnej pôsobnosti uplatňovania všeobecného nariadenia o ochrane údajov a jeho pojmom „osobné údaje“, „pseudonymizácia“ a „anonymizované informácie“.

50. Podľa článku 28-7 zákona o ochrane osobných informácií sa však články 20, 21, 27, článok 34 ods. 1, články 35 až 37, články 39-3, 39-4, články 39-6 až 39-8 na pseudonymizované informácie nevzťahujú.

51. Európska komisia vo svojom návrhu rozhodnutia uvádza, že článok 28-7 zákona o ochrane osobných informácií sa na pseudonymizované osobné informácie vzťahuje len vtedy, keď sa spracúvajú na účely štatistiky, vedeckého výskumu či archivácie vo verejnom záujme[19]. To však nevyplýva priamo zo znenia zákona, ale z vysvetlení uvedených v oznámení č. 2021-1[20]. Hoci EDPB uznáva, že na základe štruktúry a odôvodnení zákona o ochrane osobných informácií možno argumentovať, že článok 28-2 zákona o ochrane osobných informácií by sa mal chápať a logicky vykladať tak, že sa vzťahuje aj na článok 28-7 tohto zákona, EDPB vzhľadom na význam oznámenia č. 2021-1 z hľadiska posúdenia primeranosti úrovne ochrany osobných údajov v Kórejskej republike, ktoré vykonala Európska komisia, a s cieľom predísť akýmkoľvek pochybnostiam vyzýva Európsku komisiu, aby poskytla ďalšie informácie o záväznej povahe, vykonateľnosti a platnosti oznámenia č. 2021-1 a monitorovala jeho uplatňovanie v tomto osobitnom kontexte.

52. EDPB by v tejto súvislosti chcel pripomenúť, že pseudonymizácia sa podľa všeobecného nariadenia o ochrane údajov chápe ako odporúčané bezpečnostné opatrenie. Inými slovami, pseudonymizované údaje podľa všeobecného nariadenia o ochrane údajov sú aj naďalej osobnými údajmi, na ktoré sa všeobecné nariadenie o ochrane údajov vzťahuje v plnej miere. Na základe uvedených skutočností EDPB vyjadruje znepokojenie, že úroveň ochrany pseudonymizovaných osobných údajov podľa všeobecného nariadenia o ochrane údajov by mohla byť pri prenose osobných údajov do Kórey ohrozená. EDPB preto vyzýva Európsku komisiu, aby ďalej posúdila dôsledky pseudonymizácie podľa zákona o ochrane osobných informácií a predovšetkým spôsob, akým to môže ovplyvniť základné práva a slobody dotknutých osôb, ktorých osobné údaje by sa na základe rozhodnutia o primeranosti prenášali do Kórejskej republiky. EDPB teda vyzýva Európsku komisiu, aby poskytla záruky, že úroveň ochrany osobných údajov dotknutých osôb v EHP sa po prenose do Kórejskej republiky nezníži, a to ani keď budú prenášané pseudonymizované osobné údaje.

3.1.1.2. *Pojem „prevádzkovateľ osobných informácií“*

53. V článku 2 ods. 5 zákona o ochrane osobných informácií sa nachádza vymedzenie pojmu „prevádzkovateľ osobných informácií“, čo predstavuje verejnú inštitúciu, právnickú osobu, organizáciu alebo fyzickú osobu atď., ktorá *„v rámci svojej činnosti“* priamo alebo nepriamo spracúva osobné informácie pri vedení zložiek osobných informácií. V dodatočných zárukách stanovených v oznámení č. 2021-1 sa pojem „prevádzkovateľ osobných informácií“ však vymedzuje ako verejná inštitúcia, právnická osoba, organizácia, fyzická osoba atď., ktorá pri vedení zložiek osobných informácií priamo alebo nepriamo spracúva osobné informácie *„na obchodné účely“*. Namiesto toho sa v poznámke pod čiarou č. 272 pri pojme „prevádzkovateľ osobných informácií“ uvádza tento text: *„Ako sa vymedzuje v článku 2 zákona o ochrane osobných informácií, t. j. verejná inštitúcia, právnická*

[19] Pozri aj odôvodnenie 82 návrhu rozhodnutia.
[20] Oddiel 4 prílohy I k návrhu rozhodnutia.

osoba, organizácia, fyzická osoba atď., ktorá priamo alebo nepriamo spracúva osobné informácie pri vedení zložiek osobných informácií na ‚úradné alebo obchodné účely'."

54. EDPB uznáva, že tieto nezrovnalosti mohli vzniknúť pri prekladoch pôvodného textu, ktoré poskytli kórejské orgány, a vyzýva Európsku komisiu, aby pravidelne overovala kvalitu a výstižnosť prekladov. EDPB však zdôrazňuje túto skutočnosť – aby bolo možné posúdiť podstatnú rovnocennosť úrovne ochrany údajov zabezpečenej kórejským právnym rámcom, vyžaduje sa jasné pochopenie účelov spracúvania, ktoré patria do vecnej pôsobnosti zákona o ochrane osobných informácií. EDPB okrem toho v tejto súvislosti konštatuje, že zákon o ochrane osobných informácií nepoužíva rovnakú terminológiu ako všeobecné nariadenie o ochrane údajov, pokiaľ ide o pojem „prevádzkovateľ" a „sprostredkovateľ", a vyzýva Európsku komisiu, aby objasnila správne vymedzenie a rozsah pôsobnosti pojmu „prevádzkovateľ osobných informácií" a osobitne sa zamerala na to, či sa tento pojem vzťahuje aj na sprostredkovateľov v zmysle všeobecného nariadenia o ochrane údajov, keďže to má priamy vplyv na rozsah pôsobnosti rozhodnutia o primeranosti[21].

3.1.2. Čiastočné výnimky stanovené v zákone o ochrane osobných informácií

55. V článku 58 ods. 1 zákona o ochrane osobných informácií sa vylučuje uplatňovanie častí tohto zákona (t. j. článkov 15 až 57) na štyri kategórie spracúvania osobných údajov uvedené ďalej v texte. Výnimky sa konkrétne týkajú ustanovení zákona o ochrane osobných informácií o osobitných dôvodoch na spracúvanie, určitých povinnostiach v oblasti ochrany údajov, podrobných pravidlách na uplatnenie individuálnych práv, ako aj ustanovení upravujúcich riešenie sporov. EDPB však konštatuje, že niektoré všeobecné ustanovenia zákona o ochrane osobných informácií sú aj naďalej uplatniteľné, napríklad ustanovenia týkajúce sa zásad ochrany údajov (článok 3 zákona) a individuálne práva (článok 4 zákona). Navyše v článku 58 ods. 4 zákona o ochrane osobných informácií sa stanovujú osobitné povinnosti v prípade daných štyroch kategórií spracúvania údajov.

56. Prvá čiastočná výnimka sa vzťahuje na osobné informácie získané podľa zákona o štatistike na účely spracúvania vykonávaného verejnými inštitúciami. Európska komisia v odôvodnení 27 svojho návrhu rozhodnutia uvádza, že podľa objasnení získaných od kórejskej vlády sa osobné údaje spracúvané v tomto kontexte zvyčajne týkajú kórejských štátnych príslušníkov a informácie o cudzích štátnych príslušníkoch môžu zahŕňať len vo výnimočných prípadoch, konkrétne ak ide o štatistiky o vstupe na územie a odchode z neho alebo o zahraničné investície. V návrhu rozhodnutia sa však uvádza, že ani v týchto situáciách sa uvedené údaje zvyčajne neprenášajú od prevádzkovateľov/sprostredkovateľov v EHP, ale skôr ich orgány verejnej moci v Kórei získavajú priamo.

57. EDPB berie na vedomie odôvodnenie Európskej komisie týkajúce sa výnimočných prípadov uplatňovania zákona o štatistike na spracúvanie osobných údajov prenášaných na základe rozhodnutia o primeranosti; uvítal by však ďalšie informácie a uistenia o osobitných zárukách, ktoré by sa uplatňovali v prípade, že by sa osobné údaje prenášané z EHP ďalej získavali v súlade so zákonom o štatistike na spracúvanie verejnými inštitúciami, najmä v súvislosti s uplatnením individuálnych práv dotknutých osôb v súlade s článkom 89 ods. 2 všeobecného nariadenia o ochrane údajov, pokiaľ takéto práva pravdepodobne neznemožnia alebo závažným spôsobom nesťažia dosiahnutie osobitných účelov a pokiaľ takéto odchýlky nie sú nevyhnutné na splnenie uvedených účelov.

58. Z tohto hľadiska sa javí, že uplatňovaním článku 4 zákona o ochrane osobných informácií aj na tento druh spracúvania sa poskytujú uistenia, EDPB by však v rozhodnutí o primeranosti uvítal dodatočné informácie a objasnenia týkajúce sa uložených osobitných povinností v súlade s článkom 58 ods. 4 zákona o ochrane osobných informácií, pokiaľ ide o uvedené spracovateľské činnosti, konkrétne o minimalizáciu údajov, obmedzené uchovávanie údajov, bezpečnostné opatrenia a vybavovanie sťažností.

[21] Pozri aj bod 38.

59. Druhá čiastočná výnimka sa vzťahuje na osobné informácie získané alebo vyžiadané na účely analýzy informácií súvisiacich s národnou bezpečnosťou. EDPB si uvedomuje skutočnosť, že v záležitostiach národnej bezpečnosti majú štáty k dispozícii široký priestor na voľnú úvahu priznaný ESĽP. EDPB takisto berie na vedomie, že podľa článku 37 ods. 2 kórejskej ústavy sa žiadnym obmedzením slobôd a práv, napríklad v prípade potreby ochrany národnej bezpečnosti, nemôže porušiť základný aspekt daného práva alebo slobody. Ďalej EDPB berie na vedomie záruky v oddiele 6 oznámenia č. 2021-1 týkajúce sa spracúvania osobných informácií na účely národnej bezpečnosti, a to aj pri vyšetrovaní porušení a presadzovaní práva. EDPB však v tomto kontexte vyzýva Európsku komisiu, aby bližšie objasnila rozsah uplatňovania výnimiek, keďže sa zamýšľa, či sú všetky výnimky stanovené v článku 58 ods. 1 pododseku 2 zákona o ochrane osobných informácií (kapitoly III až VII) relevantné z hľadiska činnosti spravodajských služieb a či sa nimi zabezpečuje rovnocennosť so zásadami nevyhnutnosti a proporcionality. EDPB vyzýva Európsku komisiu, aby konkrétne poskytla bližšie objasnenie v súvislosti s okolnosťami, za ktorých by sa spravodajská služba mohla o tieto výnimky opierať. EDPB to považuje za nevyhnutné na dôkladné monitorovanie vplyvu týchto obmedzení v praxi, obzvlášť účinného uplatňovania a presadzovania práv dotknutých osôb.

60. Tretia čiastočná výnimka sa vzťahuje na „*osobné informácie spracúvané dočasne v prípade naliehavej potreby zaistenia verejnej ochrany a bezpečnosti, verejného zdravia atď.*“ Európska komisia v odôvodnení 29 návrhu rozhodnutia uvádza, že túto kategóriu vykladá striktne Komisia pre ochranu osobných informácií a uplatňuje sa len v núdzových situáciách, ktoré si vyžadujú prijatie naliehavých krokov, ako je sledovanie infekčných mikroorganizmov alebo záchrana a poskytnutie pomoci obetiam živelných pohrôm.

61. EDPB okrem toho zdôrazňuje, že každá odchýlka z úrovne ochrany osobných údajov by sa mala vykladať striktne. EDPB zároveň konštatuje, že ustanovenie nie je striktne vymedzené a neuvádza podrobný zoznam príkladov situácií, v ktorých možno spracúvanie osobných informácií považovať za prípad „*naliehavej potreby*“. EDPB vyjadruje znepokojenie napríklad nad tým, či by do rozsahu uplatňovania tejto výnimky takisto patrili medzinárodné prenosy zdravotných údajov počas prebiehajúcej pandémie COVID-19. Vzhľadom na uvedené skutočnosti EDPB vyzýva Európsku komisiu, aby poskytla ďalšie objasnenia rozsahu uplatňovania tejto výnimky a dôkladne monitorovala jej uplatňovanie (vrátane rozsahu) v záujme zaistenia, že nepovedie k zníženiu úrovne ochrany osobných údajov z EHP po ich prenose do Kórey na základe rozhodnutia o primeranosti.

62. A napokon posledná čiastočná výnimka sa vzťahuje na osobné informácie získané alebo použité na účely podávania správ tlačou, vykonávanie misijných činností náboženskými organizáciami a vymenovanie kandidátov politickými stranami[22]. Pokiaľ ide o spracúvanie osobných informácií tlačou na účely žurnalistickej činnosti, Európska komisia v odôvodnení 31 svojho návrhu rozhodnutia uvádza, že vyváženie práva na slobodu prejavu a ďalších práv vrátane práva na súkromie je stanovené v zákone o rozhodcovskom konaní a prostriedkoch nápravy atď. v prípade škody spôsobenej tlačovými správami, a predstavuje osobitné záruky, ktoré z tohto zákona vyplývajú. EDPB by však Európsku komisiu vyzval, aby dôkladne monitorovala túto výnimku a príslušnú judikatúru s cieľom zabezpečiť zaručenie rovnocennej úrovne ochrany údajov v kórejskom právnom rámci aj v praxi.

3.1.3. Dôvody zákonného a spravodlivého spracúvania na legitímne účely

63. Podľa referenčného kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov sa údaje musia v súlade so všeobecným nariadením o ochrane údajov spracúvať zákonným, spravodlivým a legitímnym spôsobom. Právny základ, podľa ktorého možno osobné údaje zákonne, spravodlivo a legitímne spracúvať, by sa mal stanoviť dostatočne jasným spôsobom. V európskom rámci sa uznáva

[22] V súlade s uvedenými skutočnosťami sa z rozsahu pôsobnosti rozhodnutia o primeranosti takisto vylučuje spracúvanie osobných informácií náboženskými organizáciami na účely ich misijných činností a spracúvanie osobných informácií politickými stranami v kontexte vymenovania kandidátov. Pozri aj bod 37 v oddiele 2.3.2.

niekoľko takýchto legitímnych dôvodov, ako sú napríklad ustanovenia vo vnútroštátnych právnych predpisoch, súhlas dotknutej osoby, plnenie zmluvy alebo oprávnený záujem prevádzkovateľa alebo tretej strany, ktorý neprevažuje nad záujmami dotknutej osoby.

64. Zákon o ochrane súkromných informácií má podobnú štruktúru ako všeobecné nariadenie o ochrane údajov, takže na začiatku sa v ňom uvádza zásada zákonnosti, spravodlivosti a transparentnosti (článok 3 ods. 1 a 2 zákona), pričom osobitné pravidlá uplatňovania tejto zásady sa stanovujú ďalej (články 15 až 19 zákona). Konkrétne v článku 15 zákona o ochrane osobných informácií sa nachádza zoznam právnych dôvodov, z ktorých môžu prevádzkovatelia osobných informácií vychádzať pri získavaní osobných informácií a využívať ich v rozsahu účelu ich získavania. Týmito právnymi dôvodmi sú: 1. informovaný súhlas dotknutej osoby; 2. oprávnenie zo zákona alebo potreba plniť zákonnú povinnosť; 3. potreba plniť povinnosti verejnej inštitúcie; 4. potreba vykonávať alebo plniť zmluvu, ktorej zmluvnou stranou je dotknutá osoba; 5. potreba chrániť záujmy dotknutej osoby alebo tretej strany, ktoré sa týkajú jej života, fyzickej integrity a majetku, pred bezprostredným nebezpečenstvom (a ich súhlas nemožno získať vopred); 6. potreba dosiahnuť odôvodnený [justifiable] záujem prevádzkovateľa osobných informácií, ktorý je nadradený záujmom dotknutej osoby.

65. V článku 17 zákona o ochrane osobných informácií sa navyše uvádza zoznam právnych dôvodov na poskytnutie osobných informácií tretej strane, konkrétne: 1. informovaný súhlas dotknutej osoby; 2. oprávnenie zo zákona alebo potreba plniť zákonnú povinnosť; 3. potreba plniť povinnosti verejnej inštitúcie; a 4. potreba chrániť záujmy dotknutej osoby alebo tretej strany, ktoré sa týkajú jej života, fyzickej integrity a majetku, pred bezprostredným nebezpečenstvom (a ich súhlas nemožno získať vopred). Aj v prípade, že dotknutá osoba nevyjadrila súhlas, je možné poskytnúť jej osobné údaje, ak sa tak udeje v rozsahu, ktorý primerane súvisí s účelmi, na ktoré sa osobné informácie pôvodne získali (článok 17 ods. 4 zákona o ochrane osobných informácií).

66. V článku 18 zákona o ochrane osobných informácií sa stanovujú osobitné pravidlá využívania a poskytovania osobných údajov, ak sa tak udeje mimo rozsahu pôvodného účelu získavania a poskytovania. Aj v tomto prípade je súhlas jedným z oprávňujúcich pravidiel.

67. Hoci EDPB uznáva značnú podobnosť kórejskej právnej úpravy a všeobecného nariadenia o ochrane údajov, pokiaľ ide o zásadu zákonnosti a existenciu všeobecného práva na pozastavenie spracúvania (článok 37 zákona o ochrane osobných informácií), na ktoré sa možno odvolávať aj v prípade, že sa osobné údaje spracúvajú na základe súhlasu, chcel by poznamenať, že podľa zákona o ochrane osobných informácií neexistuje všeobecné právo odvolať súhlas[23]. Vzhľadom na význam súhlasu ako právneho dôvodu vo všetkých uvedených situáciách a vzhľadom na úlohu individuálnych práv stanovených v právnom systéme ochrany údajov na účely ochrany základných práv a slobôd dotknutej osoby EDPB vyzýva Európsku komisiu, aby ďalej posúdila dôsledky neexistencie všeobecného práva odvolať súhlas podľa kórejského práva a poskytla ďalšie záruky, a tak zabezpečila úroveň ochrany údajov, ktorá je rovnocenná úrovni ochrany zaručenej všeobecným nariadením o ochrane údajov, za každých okolností, prípadne aj objasnením úlohy práva na pozastavenie spracúvania v tomto konkrétnom kontexte.

[23] Hoci dotknuté osoby za istých okolností môžu odoprieť súhlas, pozri napríklad článok 18 ods. 3 pododsek 5 zákona o ochrane osobných informácií. Naopak, zdá sa, že právo odvolať súhlas existuje iba v osobitných prípadoch; podľa článku 27 ods. 1 pododseku 2 zákona o ochrane osobných informácií majú dotknuté osoby právo odvolať súhlas, ak si neželajú, aby sa ich osobné údaje prenášali tretej strane z dôvodu prevodu časti alebo celej obchodnej činnosti prevádzkovateľa osobných informácií, zlúčenia atď.; podľa článku 39-7 zákona o ochrane osobných informácií môžu používatelia kedykoľvek odvolať súhlas so získavaním, s využívaním a poskytovaním osobných informácií u poskytovateľa informačných a komunikačných služieb atď.; a podľa článku 37 zákona o používaní a ochrane úverových informácií môže individuálna osoba, ktorej sa týkajú úverové informácie, odvolať súhlas, ktorý poskytla poskytovateľovi/používateľovi úverových informácií.

3.1.4. Zásada obmedzenia účelu

68. V referenčnom kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov sa v súlade so všeobecným nariadením o ochrane údajov stanovuje, že osobné údaje by sa mali spracúvať na konkrétny účel a následne by sa mali použiť len vtedy, keď to nie je nezlučiteľné s účelom spracúvania.

69. Podľa článku 3 ods. 1 a 2 zákona o ochrane osobných informácií prevádzkovatelia osobných informácií výslovne spresnia účely spracúvania a zabezpečia, že spracúvanie je zlučiteľné s týmito účelmi. Hoci je táto zásada potvrdená v iných ustanoveniach (t. j. v článku 15 ods. 1, článku 18 ods. 1 a článku 19 ods. 1 zákona o ochrane osobných informácií), spracúvanie na účely, ktoré „primerane súvisia“, je za určitých okolností povolené (pozri článok 17 ods. 4 zákona o ochrane osobných informácií)[24], ako aj používanie a poskytovanie osobných informácií mimo stanoveného účelu (pozri články 18 a 19 zákona o ochrane osobných informácií)[25].

70. EDPB chápe, že v prípade prenosov osobných údajov z EHP do Kórejskej republiky na základe rozhodnutia o primeranosti, účel získavania prevádzkovateľov so sídlom v EHP tvorí účel, na ktorý sa údaje prenášajú na spracúvanie prijímajúcim prevádzkovateľom osobných informácií so sídlom v Kórei. Zmena účelu prevádzkovateľom so sídlom v Kórei by bola povolená len za okolností stanovených v článku 18 ods. 2 pododsekoch 1 až 3 zákona o ochrane osobných informácií, „*ak nie je pravdepodobné, že by sa tým nespravodlivo poškodil záujem dotknutej osoby alebo tretej strany*“[26]. EDPB v tejto súvislosti uznáva vyhlásenie Európskej komisie v odôvodnení 55 návrhu rozhodnutia, kde sa uvádza, že ak zmeny účelu podľa zákonov možno oprávnene vykonať, v týchto zákonoch sa musí dodržiavať základné právo na súkromie a ochranu údajov. EDPB však konštatuje, že na podporu tohto konkrétneho vyhlásenia sa neposkytli žiadne osobitné informácie, napr. sa neuviedol odkaz na článok 37 (kórejskej) ústavy. EDPB preto vyzýva Európsku komisiu, aby v návrhu rozhodnutia poskytla ďalšie uistenia a záruky na zabezpečenie, že v každom zákone, na základe ktorého možno oprávnene vykonať zmenu účelu spracúvania, sa musia dodržiavať základné práva a slobody dotknutých osôb v oblasti súkromia a ochrany údajov.

3.1.5. Zásada kvality údajov a zásada proporcionality

71. V referenčnom kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov sa uvádza, že údaje by mali byť správne a podľa potreby aktualizované. Údaje by mali byť primerané, relevantné a nie neúmerné vo vzťahu k účelom, na ktoré sa spracúvajú.

72. Podľa zákona o ochrane osobných informácií musia prevádzkovatelia osobných informácií zabezpečiť správnosť, úplnosť a aktuálnosť osobných informácií v rozsahu potrebnom na účely, na ktoré sa osobné informácie spracúvajú (článok 3 ods. 3 zákona o ochrane osobných informácií). Od prevádzkovateľov osobných informácií sa vyžaduje, aby získavali čo najmenšie množstvo osobných informácií v rozsahu, aký je potrebný na dosiahnutie daného účelu. V tejto súvislosti znášajú dôkazné bremeno (článok 16 ods. 1 zákona o ochrane osobných informácií).

73. Na základe uvedených skutočností sa EDPB stotožňuje s posúdením Európskej komisie, pokiaľ ide o podstatnú rovnocennosť úrovne ochrany podľa zákona o ochrane osobných informácií vo vzťahu k všeobecnému nariadeniu o ochrane údajov v tejto súvislosti.

3.1.6. Zásada uchovávania údajov

74. Podľa referenčného kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov by sa údaje vo všeobecnosti nemali uchovávať dlhšie, než je potrebné na účely, na ktoré sa osobné údaje

[24] Pričom účel zlučiteľnosti musí byť vopred stanovený na základe kritérií uvedených v článku 14-2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.
[25] Pozri aj bod 66.
[26] Článok 18 ods. 2 zákona o ochrane osobných informácií.

spracúvajú. Táto zásada sa nachádza aj v kórejskom práve, konkrétne je zavedená v článku 21 ods. 1 zákona o ochrane osobných informácií. Podľa zákona o ochrane osobných informácií sa od prevádzkovateľov osobných informácií vyžaduje, aby osobné informácie bezodkladne zničili, ak sa osobné informácie po uplynutí obdobia uchovávania alebo dosiahnutí zamýšľaného účelu spracúvania stanú nepotrebnými, pokiaľ sa zo zákona neuplatňujú obdobia uchovávania.

75. EDPB však vyjadruje znepokojenie so zreteľom na skutočnosť, že článok 21 ods. 1 zákona o ochrane osobných informácií sa nevzťahuje na pseudonymizované osobné informácie. EDPB berie na vedomie skutočnosť, že v oddiele 4 bode iii) oznámenia č. 2021-1 sa uvádza: „*Ak prevádzkovateľ osobných informácií spracúva pseudonymizované informácie na účely zostavovania štatistík, vedeckého výskumu, archivovania verejných záznamov atď. a ak pseudonymizované informácie neboli po dosiahnutí konkrétneho účelu spracúvania zničené v súlade s článkom 37 ústavy a článkom 3 (Zásady ochrany osobných informácií) zákona, anonymizuje informácie s cieľom zabezpečiť, aby sa už na ich základe nedal identifikovať konkrétny jednotlivec ani v prípade ich samostatného použitia, ani v prípade ich skombinovania s inými informáciami, pričom sa primerane prihliadne na čas, náklady, technológie atď. v súlade s článkom 58-2 zákona o ochrane osobných informácií*“. EDPB aj v tomto prípade vzhľadom na význam oznámenia č. 2021-1 a vzhľadom na existujúcu právnu istotu v súvislosti s rovnocennosťou úrovne ochrany osobných údajov prenášaných do Kórejskej republiky na základe rozhodnutia o primeranosti opakovane vyzýva Európsku komisiu, aby poskytla ďalšie informácie, konkrétne s ohľadom na to, akým spôsobom sa zaistí záväznosť, vykonateľnosť a platnosť oznámenia č. 2021-1[27].

3.1.7. Zásada bezpečnosti a dôvernosti

76. Ako sa uvádza v referenčnom kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov, na základe zásady bezpečnosti a dôvernosti sa od subjektov spracúvajúcich údaje vyžaduje, aby zabezpečili, že údaje sa spracúvajú spôsobom, ktorý zaručuje ich bezpečnosť vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení. Úroveň bezpečnosti by mala zohľadňovať najnovšie poznatky a súvisiace náklady.

77. Európska komisia zistila, že v článku 3 ods. 4 zákona o ochrane osobných informácií sa nachádza podobná zásada bezpečnosti údajov, ktorá je bližšie spresnená v článku 29 tohto zákona. Okrem toho sa ustanovenia o bezpečnosti údajov uplatňujú, ak prevádzkovateľ osobných informácií do činnosti zapojí „externého poskytovateľa spracúvania“. Bezpečnosť spracúvania musí byť zaistená pomocou technických a riadiacich záruk, ktoré navyše musia byť zahrnuté v záväznej dohode o spracúvaní údajov (článok 26 zákona o ochrane osobných informácií a článok 28 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Ďalej, ak dôjde k porušeniu ochrany údajov, podľa zákona o ochrane osobných informácií sa uplatňujú osobitné povinnosti vrátane povinnosti informovať dotknuté osoby, v prípade ktorých došlo k takému porušeniu, a dozorný orgán, ak počet dotknutých osôb, v prípade ktorých došlo k takému porušeniu, prekročí príslušnú prahovú hodnotu (článok 34 zákona o ochrane osobných informácií v spojení s článkom 39 prezidentského dekrétu k zákonu o ochrane osobných informácií), pričom sa uplatňuje výnimka, ak sú údaje, v prípade ktorých došlo k porušeniu ochrany, pseudonymizovanými osobnými informáciami spracúvanými na účely štatistiky, vedeckého výskumu či archivácie vo verejnom záujme (článok 28-7 zákona o ochrane osobných informácií). Aj v tomto prípade[28] EDPB vyjadruje znepokojenie nad širokým rozsahom uplatňovania výnimiek týkajúcich sa

[27] Pozri aj bod 51 v oddiele 3.1.1.1 tohto stanoviska, ako aj bod 52 v súvislosti so všeobecnými obavami EDPB týkajúcimi sa dôsledkov pseudonymizácie podľa kórejského práva.
[28] Ako sa už uvádza v bodoch 51 až 52 a v oddiele 3.1.1.1 tohto stanoviska.

pseudonymizovaných informácií a opakovane vyzýva Európsku komisiu, aby ďalej posúdila tento aspekt, a tak zabezpečila, že v kórejskom práve je stanovená v podstate rovnocenná úroveň ochrany[29].

78. Napriek uvedeným skutočnostiam EDPB celkovo vyjadruje spokojnosť s posúdením a so záverom Európskej komisie, pokiaľ ide o podstatnú rovnocennosť zásady bezpečnosti a dôvernosti stanovenej v kórejskom práve.

3.1.8. Zásada transparentnosti

79. Na základe článku 5 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov je transparentnosť základnou zásadou systému ochrany údajov v EÚ. V odôvodnení 39 všeobecného nariadenia o ochrane údajov sa opisuje kľúčová funkcia tejto zásady uvedením, že „*[p]re fyzické osoby by malo byť transparentné, že sa získavajú, používajú, konzultujú alebo inak spracúvajú osobné údaje, ktoré sa ich týkajú, ako aj to, v akom rozsahu sa tieto osobné údaje spracúvajú alebo budú spracúvať. (…) Fyzické osoby by mali byť upozornené na riziká, pravidlá, záruky a práva pri spracúvaní osobných údajov, ako aj na to, ako uplatňovať svoje práva pri takomto spracúvaní.*“

80. V referenčnom kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov sa „transparentnosť“ výslovne označuje za jednu zo zásad obsahu, ktoré sa majú brať do úvahy pri hodnotení podstatnej rovnocennosti úrovne ochrany poskytovanej treťou krajinou. Konkrétne sa v ňom uvádza, že „*[k]ažd*ý *jednotlivec by mal byť informovaný o všetkých hlavných prvkoch spracúvania jeho osobných údajov, a to jasným, ľahko dostupným, stručným, transparentným a zrozumiteľným spôsobom. Takéto informácie by mali zahŕňať účel spracúvania, totožnosť prevádzkovateľa, práva, ktoré má k dispozícii, a iné informácie, pokiaľ je to nevyhnutné na zabezpečenie spravodlivosti. Za určitých podmienok môžu existovať niektoré výnimky z tohto práva na informácie, napríklad keď ide o ochranu trestného vyšetrovania, národnú bezpečnosť, nezávislosť súdov a súdne konania alebo iné dôležité ciele všeobecného verejného záujmu, ako je to v prípade článku 23 všeobecného nariadenia o ochrane údajov.*“

81. Podobne ako je to v prípade všeobecného nariadenia o ochrane údajov, v zákone o ochrane osobných informácií sa nachádza všeobecná zásada transparentnosti, na základe ktorej sa od prevádzkovateľov osobných informácií vyžaduje, aby zverejňovali svoju politiku súkromia, ako aj iné záležitosti týkajúce sa spracúvania osobných informácií (článok 3 ods. 5 zákona o ochrane osobných informácií). Ak sa prevádzkovatelia osobných informácii usilujú získať od dotknutých osôb súhlas na získavanie a spracúvanie osobných informácií (článok 15 ods. 2 zákona o ochrane osobných informácií), na poskytnutie osobných informácií tretej strane (článok 17 ods. 2 zákona o ochrane osobných informácií) a na spracúvanie mimo stanoveného účelu (článok 18 ods. 3 zákona o ochrane osobných informácií), uplatňujú sa osobitné povinnosti poskytovania informácií. Treba poznamenať, že tieto povinnosti poskytovania informácií sa vzťahujú *mutatis mutandis* aj na externého poskytovateľa spracúvania (článok 26 ods. 7 zákona o ochrane osobných informácií).

82. EDPB uznáva a víta dodatočné záruky uvedené v oddiele 3 bodoch i) a ii) oznámenia č. 2021-1[30] týkajúce sa informácií, ktoré sa majú poskytnúť dotknutým osobám pri prenose ich údajov subjektom v EHP, pričom zohľadňuje skutočnosť, že podľa článku 20 ods. 1 zákona o ochrane osobných informácií, ak sa údaje od dotknutej osoby nezískali, dotknuté osoby sú informované len na požiadanie, zatiaľ čo všeobecné právo byť informovaný sa uznáva len podľa článku 20 ods. 2 zákona o ochrane osobných informácií, ak určité spracovateľské operácie prekračujú prahové hodnoty stanovené vo vykonávacom dekréte k zákonu o ochrane osobných informácií (článok 15 ods. 2).

[29] Pozri aj oddiely 3.1.6 a 3.1.10 tohto stanoviska.
[30] Pozri prílohu I k návrhu rozhodnutia.

83. EDPB celkovo vyjadruje spokojnosť s tým, že úroveň ochrany v súvislosti so zásadou transparentnosti stanovená v kórejskom práve je v podstate rovnocenná s úrovňou ochrany zaručenou GDPR.

3.1.9. Osobitné kategórie osobných údajov

84. Na to, aby sa systém ochrany údajov tretej krajiny mohol uznať za systém poskytujúci úroveň ochrany osobných údajov, ktorá je v podstate rovnocenná s úrovňou ochrany zaručenou všeobecným nariadením o ochrane údajov, by mali v prípade osobitných kategórií osobných údajov v zmysle článkov 9 a 10 všeobecného nariadenia o ochrane údajov existovať osobitné záruky.

85. Podľa zákona o ochrane osobných informácií sa osobitné ustanovenia vzťahujú na spracúvanie tzv. citlivých informácií, ktoré zahŕňajú osobné informácie odhaľujúce ideológiu, presvedčenie, vstup do odborovej organizácie alebo politickej strany alebo vystúpenie z nich, politické názory, zdravie, sexuálny život a iné osobné informácie, ktoré s pravdepodobnosťou môžu výrazne ohroziť súkromie akejkoľvek dotknutej osoby, a zároveň podľa vykonávacieho dekrétu k zákonu o ochrane osobných informácií aj na informácie o DNA získané z genetického testovania, údaje, ktoré predstavujú záznam v registri trestov; osobné informácie, ktoré sú výsledkom osobitného technického spracúvania údajov týkajúcich sa fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby na účely individuálnej identifikácie tejto osoby; a osobné údaje odhaľujúce rasový alebo etnický pôvod.

86. Podobne, ako sa stanovuje vo všeobecnom nariadení o ochrane údajov, podľa kórejských právnych predpisov o ochrane údajov je spracúvanie citlivých informácií zakázané, pokiaľ sa neuplatňujú osobitné výnimky: 1. informovanie dotknutej osoby a získanie osobitného súhlasu; a 2. právne ustanovenia, na základe ktorých sa oprávňuje spracúvanie (článok 23 ods. 2 zákona o ochrane osobných informácií).

87. Na základe uvedených skutočností EDPB v podstate súhlasí so záverom Európskej komisie uvádzajúcim podstatnú rovnocennosť kórejského práva, pokiaľ ide o spracúvanie osobitných kategórií osobných údajov. EDPB by však chcel poznamenať, že v súvislosti s výkladom pojmu „sexuálny život“, ktorý by zahŕňal aj sexuálnu orientáciu alebo preferencie fyzickej osoby, nemal k dispozícii príručku k zákonu o ochrane osobných informácií ani objasnenia Komisie pre ochranu osobných informácií, pričom takýto výklad nebol zahrnutý v oznámení č. 2021-1. EBPD preto vyzýva Európsku komisiu, aby poskytla tieto informácie, na základe ktorých by to mohol nezávisle posúdiť. EDPB ďalej vyzýva Európsku komisiu, aby citovala konkrétne dokumenty, kde možno na túto tému nájsť informácie, na ktoré odkazuje.

3.1.10. Právo na prístup, opravu, vymazanie a právo namietať

88. V kórejskom právnom rámci sa dotknutým osobám priznávajú práva v článku 3 ods. 5 zákona o ochrane osobných informácií, podľa ktorého prevádzkovateľ osobných informácií zaručuje práva dotknutej osoby uvedené v článku 4 zákona o ochrane osobných informácií a bližšie spresnené v článkoch 35 až 37, článku 39 a článku 39-2 zákona o ochrane osobných informácií. „Osobné úverové informácie“ (t. j. úverové informácie, teda informácie, ktoré sú potrebné na určenie úverovej bonity strán finančnej alebo obchodnej transakcie – pozri odôvodnenie 3 návrhu rozhodnutia) sú stanovené v článkoch 37, 38 a 38-3 zákona o používaní a ochrane úverových informácií.

89. EDPB berie na vedomie, že právo na prístup (opravu a vymazanie, ktoré môže vykonať „*dotknutá osoba, ktorá získala prístup k svojim osobným informáciám v súlade s článkom 35“* zákona o ochrane osobných informácií) sa môže obmedziť alebo zamietnuť, „*ak je získanie prístupu zakázané alebo obmedzené zákonmi*“, „*ak získanie prístupu môže spôsobiť ohrozenie života alebo fyzickej integrity tretej strany, prípadne neopodstatnené poškodenie majetku a iných záujmov akejkoľvek inej osoby*“, a navyše v prípade verejných inštitúcií, ak by udelenie prístupu „*spôsobilo závažné ťažkosti*“ pri vykonávaní určitých funkcií, ktoré sú bližšie spresnené v článku 35 ods. 4 zákona o ochrane osobných

informácií[31]. V článku 37 zákona o ochrane osobných informácií sú zahrnuté aj podobné ustanovenia týkajúce sa práva na pozastavenie spracúvania osobných informácií.

90. Na základe článku 23 všeobecného nariadenia o ochrane údajov sa umožňuje v práve Únie alebo členského štátu obmedziť individuálne práva, ak takéto obmedzenie rešpektuje podstatu základných práv a slobôd a je nevyhnutným a primeraným opatrením v demokratickej spoločnosti a zároveň počíta s tým, že takéto obmedzenia okrem iného zaistia ochranu dotknutej osoby alebo práv a slobôd iných, ako aj „*monitorovaciu, kontrolnú alebo regulačnú funkciu spojenú, hoci aj príležitostne, s výkonom verejnej moci v prípadoch uvedených v písmenách a) až e) a g)*“ rovnakého článku.

91. V tejto súvislosti by EDPB v návrhu rozhodnutia uvítal všeobecné uistenia týkajúce sa potreby právnej úpravy alebo zákona, ktorým sa obmedzia práva dotknutých osôb plniť požiadavky stanovené kórejskou ústavou, a to že základné právo možno obmedziť len vtedy, ak je to potrebné z dôvodu národnej bezpečnosti alebo udržania verejného poriadku pre blaho verejnosti, pričom toto obmedzenie nesmie ovplyvňovať podstatu dotknutej slobody alebo práva (článok 37 ods. 2 kórejskej ústavy).

92. Okrem toho, pokiaľ ide o výnimku týkajúcu sa „*neopodstatneného poškodenia majetku a iných záujmov akejkoľvek inej osoby*“, EDPB uznáva, že na základe toho „*sa predpokladá, že by sa mali vyvážiť práva a slobody fyzickej osoby chránené ústavou na jednej strane a takéto práva a slobody iných osôb na strane druhej*“[32], vyzýva však Európsku komisiu, aby dôkladne monitorovala uplatňovanie tejto výnimky a príslušnú judikatúru s cieľom zabezpečiť zaručenie rovnocennej úrovne ochrany práv dotknutých osôb v kórejskom právnom rámci aj v praxi.

93. EDPB by rovnako uvítal dôkladné monitorovanie uplatňovania výnimky v prípade verejných inštitúcií, najmä pokiaľ ide o prípady, keď by sa udelenie prístupu považovalo za príčinu spôsobujúcu „*závažné ťažkosti*“ pri plnení ich povinností, pričom sa prihliada na to, že tento výraz sa javí rozsiahlejší než výraz, ktorý sa používa v iných ustanoveniach zákona o ochrane súkromných informácií, napr. v článku 18 ods. 2 pododseku 5[33], a mal by sa vykladať reštriktívne, aby sa predišlo neprimeraným obmedzeniam práv dotknutých osôb.

94. EDPB navyše vyjadruje znepokojenie nad tým, či výnimky, podľa ktorých sa ustanovenia týkajúce sa žiadosti v súvislosti s transparentnosťou (článok 20 zákona o ochrane osobných informácií) a individuálnych práv (články 35 až 37 zákona o ochrane osobných informácií), ako aj podobné ustanovenia týkajúce sa požiadaviek na poskytovateľov informačných a komunikačných služieb (článok 39-2, článok 39-6 až článok 39-8 zákona o ochrane osobných informácií) a ustanovenia zahrnuté do zákona o ochrane a používaní úverových informácií (pozri výnimky uvedené v článku 40 ods. 3 zákona o používaní a ochrane úverových informácií) nevzťahujú na pseudonymizované informácie, ak sa takéto informácie spracúvajú na účely štatistiky, vedeckého výskumu či archivácie vo verejnom záujme (článok 28-7 zákona o ochrane osobných informácií) a sú v súlade so zárukami stanovenými v európskom právnom rámci.

95. Zdá sa, že týmito ustanoveniami sa zavádza všeobecná odchýlka takéhoto spracúvania, zatiaľ čo v GDPR sa uvádza, že keď sa osobné údaje (vrátane pseudonymizovaných osobných údajov) spracúvajú na účely vedeckého alebo historického výskumu či na štatistické účely, v práve Únie alebo v práve členského štátu sa môžu stanoviť odchýlky z práv dotknutých osôb, ale iba „ *pokiaľ takéto*

[31] Rovnaké podmienky a výnimky týkajúce sa práva na prístup a opravu, ktoré sa uvádzajú v zákone o ochrane osobných informácií, sa uplatňujú aj v prípade práva na prístup a opravu osobných úverových informácií, ktoré sú uvedené v zákone o používaní a ochrane úverových informácií (poznámka pod čiarou č. 135 návrhu rozhodnutia).

[32] Odôvodnenie 76 návrhu rozhodnutia.

[33] V súvislosti s výnimkami obmedzenia používania a poskytovania osobných informácií mimo stanoveného účelu sa v článku 18 ods. 2 pododseku 5 zákona o ochrane osobných informácií odkazuje na situácie, keď si verejné inštitúcie „*nemôžu*“ plniť povinnosti.

práva pravdepodobne znemožnia alebo závažným spôsobom sťažia dosiahnutie osobitných účelov, a takéto odchýlky sú nevyhnutné na dosiahnutie uvedených účelov“, pričom pseudonymizácia je jediným technickým a organizačným opatrením, ktoré sa má prijať s cieľom zabezpečiť dodržiavanie zásady minimalizácie údajov (článok 89 ods. 1 všeobecného nariadenia o ochrane údajov).

96. Európska komisia považuje odchýlku uvedenú v článku 28-7 zákona o ochrane osobných informácií za odôvodnenú aj so zreteľom na článok 28-5 uvedeného zákona, ktorým sa prevádzkovateľovi osobných informácií výslovne zakazuje spracúvať pseudonymizované informácie na účely identifikácie konkrétneho jednotlivca, pričom odkazuje na prístup uvedený v článku 11 ods. 2 všeobecného nariadenia o ochrane údajov (v spojení s odôvodnením 57 všeobecného nariadenia o ochrane údajov) na spracúvanie, ktoré si nevyžaduje identifikáciu[34].

97. V skutočnosti podľa článku 11 všeobecného nariadenia o ochrane údajov prevádzkovateľ nie je povinný „*uchovávať, získať alebo spracúvať dodatočné informácie na zistenie totožnosti dotknutej osoby*“ výlučne na to, aby dosiahol súlad so všeobecným nariadením o ochrane údajov, ak zamýšľané účely, na ktoré môže spracúvať osobné údaje, nevyžadujú alebo prestali vyžadovať identifikáciu dotknutej osoby; ak v takýchto prípadoch prevádzkovateľ vie preukázať, že dotknutú osobu nie je schopný identifikovať, neuplatňujú sa práva dotknutej osoby. Ako uznala Európska komisia[35], vo všeobecnom nariadení o ochrane údajov sa preto vyžaduje, aby to bolo v takýchto prípadoch pre prevádzkovateľa „prakticky“ nemožné, a v súlade so zásadou minimalizácie údajov uznáva, že sa nemusia spracúvať žiadne dodatočné údaje „z dôvodu“ všeobecného nariadenia o ochrane údajov.

98. EDPB však túto situáciu považuje za odlišnú od situácie, keď je prevádzkovateľ prakticky schopný dotknutú osobu identifikovať, ale nemôže to urobiť pre zákonné ustanovenie, ako je napríklad ustanovenie uvedené v článku 28-5 zákona o ochrane osobných informácií. V tejto súvislosti EDPB víta objasnenia, ktoré Komisia pre ochranu osobných informácií poskytla v oznámení č. 2021-1[36] a v ktorých potvrdila, že oddiel 3 zákona o ochrane osobných informácií (vrátane článku 28-7) a výnimka článku 40 ods. 3 zákona o používaní a ochrane úverových informácií sa uplatňujú iba v prípade, že sa pseudonymizované údaje spracúvajú na účely vedeckého výskumu, štatistiky či archivácie vo verejnom záujme. Napriek tomu a zároveň vzhľadom na uvedené obavy v súvislosti s účinnou záväznou povahou oznámenia č. 2021-1[37] sa EDPB naďalej zamýšľa, či by sa odchýlky uvedené v článku 28-7 zákona o ochrane osobných informácií a v článku 40 ods. 3 zákona o používaní a ochrane úverových informácií mohli považovať za potrebné a primerané v demokratickej spoločnosti, pokiaľ sa nimi obmedzujú práva dotknutých osôb vždy, keď sa pseudonymizované informácie spracúvajú na takéto účely, t. j. aj vtedy, keď je prevádzkovateľ osobných informácií prakticky schopný dotknutú osobu identifikovať a práva pravdepodobne neznemožnia alebo závažným spôsobom nesťažia dosiahnutie osobitných účelov.

99. EDPB konkrétne vyjadruje znepokojenie, že tieto odchýlky by neboli odôvodnené a vyžadovali by si ďalšie preskúmanie, obzvlášť ak by ich uplatňoval prevádzkovateľ osobných informácií, ktorý pseudonymizuje údaje „*na štatistické účely, účely vedeckého výskumu a na archivačné účely vo verejnom záujme atď.*“, v súlade s článkom 28-2 zákona o ochrane osobných informácií „*bez súhlasu dotknutých osôb*“ (a bez poskytnutia informácií uvedených v článku 20 zákona o ochrane osobných

[34] Treba poznamenať, že rovnaké odôvodnenie by sa ako také neuplatňovalo v prípade výnimky uvedenej v článku 40 ods. 3 zákona o používaní a ochrane úverových informácií na spracúvanie pseudonymizovaných úverových informácií, pretože podľa článku 40 ods. 2 pododseku 6: „*Spoločnosť pracujúca s úverovými informáciami atď. nespracúva pseudonymizované informácie spôsobom, na základe ktorého možno identifikovať konkrétneho jednotlivca na akékoľvek ziskové alebo nekalé účely*“, a preto by vďaka tomu bolo možné opätovne identifikovať jednotlivca na riadny účel, ako je napríklad vyhovenie žiadosti dotknutej osoby.

[35] Pozri odôvodnenie 82 návrhu rozhodnutia.

[36] Oddiel 4 prílohy I k návrhu rozhodnutia.

[37] Pozri oddiel 3.1.1.1.

informácií)[38], pokiaľ tento prevádzkovateľ uchováva informácie, ktoré umožňujú opätovnú identifikáciu. Na základe všeobecného nariadenia o ochrane údajov by fyzické osoby mali byť schopné uplatňovať svoje práva v súvislosti s akýmikoľvek informáciami, na základe ktorých ich možno identifikovať alebo rozpoznať, a to aj v prípade, že sa informácie považujú za „pseudonymizované“, pokiaľ sa neuplatňuje uvedený článok 11 všeobecného nariadenia o ochrane údajov. EDPB v tejto súvislosti konštatuje, že len ak sa tieto údaje poskytnú tretej strane na rovnaké štatistické účely, účely vedeckého výskumu či archivácie, by sa informácie, ktoré sa môžu použiť na identifikáciu konkrétneho jednotlivca, nemali zahŕňať, a preto by len prevádzkovateľ osobných informácií, ktorému sa v súlade s článkom 28-2 ods. 2 zákona o ochrane osobných informácií poskytujú pseudonymizované údaje, pravdepodobne „prakticky“ nebol schopný identifikovať dotknutú osobu bez dodatočných informácií.

100. Stručne povedané, vzhľadom na vyhlásenie Európskej komisie, že „*zákon o ochrane osobných informácií namiesto spoliehania sa na pseudonymizáciu ako možnú záruku ju ukladá ako podmienku na vykonanie určitých spracovateľských činností na účely štatistiky, vedeckého výskumu a archivácie vo verejnom záujme (napríklad na možnosť spracúvať údaje bez súhlasu alebo skombinovať rozličné súbory údajov)*“[39], ale v súvislosti s týmito prípadmi sa v uvedenom zákone stanovujú dôležité obmedzenia práv dotknutých osôb, EDPB vyzýva Európsku komisiu, aby ďalej posúdila odchýlky uvedené v článku 28-7 zákona o ochrane osobných informácií a článku 40 ods. 3 zákona o používaní a ochrane osobných informácií a dôkladne monitorovala ich uplatňovanie a príslušnú judikatúru[40] s cieľom zabezpečiť, že práva dotknutých osôb nebudú neprimerane obmedzené pri spracúvaní osobných údajov prenášaných na základe rozhodnutia o primeranosti na tieto účely, pričom sa zohľadní, že v mnohých prípadoch tieto práva takisto pomáhajú prevádzkovateľovi zaistiť kvalitu spracúvaných údajov.

3.1.11. Obmedzenia následných prenosov

101. V referenčnom kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov sa objasňuje, že úroveň ochrany fyzických osôb, ktorých osobné údaje sa prenášajú na základe rozhodnutia o primeranosti, nesmie byť ohrozená následným prenosom, a preto všetky následné prenosy „*by sa mali povoliť len vtedy, keď ďalší príjemca (t. j. príjemca následného prenosu) takisto podlieha pravidlám (vrátane zmluvných pravidiel), pričom má primeranú úroveň ochrany a dodržiava príslušné pokyny pri spracúvaní údajov v mene prevádzkovateľa*“.

102. Pokiaľ ide o následné prenosy externým poskytovateľom spracúvania (t. j. „sprostredkovateľom“) so sídlom v inej tretej krajine, EDPB berie na vedomie, že v kórejskom právnom rámci nie sú zavedené žiadne osobitné pravidla, ktoré by sa vzťahovali na tieto prípady, a že v súlade s konštatovaním Európskej komisie[41] musí kórejský prevádzkovateľ osobných informácií zabezpečiť dodržanie súladu s ustanoveniami zákona o ochrane osobných informácií týkajúcimi sa outsourcingu (článok 26 zákona) pomocou právne záväzného nástroja, pričom bude zodpovedný za osobné informácie, ktoré sa poskytnú v rámci outosurcingu (článok 26 zákona).

103. V súvislosti s následnými prenosmi tretím stranám (t. j. iným prevádzkovateľom osobných informácií) sa v článku 17 ods. 3 zákona o ochrane osobných informácií uvádza, že kórejský prevádzkovateľ osobných informácií musí dotknuté osoby informovať o prenose do zahraničia a získať naň ich súhlas

[38] Pozri vysvetlenie článku 28-7 zákona o ochrane osobných informácií uvedené v oznámení č. 2021-1, podľa ktorého sa určité záruky zahrnuté v zákone o ochrane osobných informácií, t. j. „*články 20, 21, 27, článok 34 ods. 1, články 35 až 37, článok 39-3, 39-4, články 39-6 až 39-8*“, nevzťahujú na pseudonymizované informácie, ktoré sa spracúvajú na účely zostavovania štatistiky, vedeckého výskumu, archivovania verejných záznamov atď.
[39] Odôvodnenie 42 návrhu rozhodnutia.
[40] Pozri napríklad ústavné problémy platformy Open Net (informácie sú k dispozícii na adrese https://opennet.or.kr/19909 iba v kórejčine).
[41] Odôvodnenie 87 návrhu rozhodnutia.

a „*neuzavrie zmluvu o cezhraničnom prenose osobných informácií, ktorý by bol v rozpore s týmto zákonom o ochrane osobných informácií*“. EDPB poznamenáva, že týmto posledným uvedeným ustanovením sa zabezpečí – v súlade s konštatovaním Európskej komisie[42] – že žiadna zmluva o cezhraničnom prenose nebude zahŕňať povinnosti, ktoré by boli v rozpore s požiadavkami uloženými prevádzkovateľovi osobných informácií zákonom o ochrane osobných informácií, a preto toto ustanovenie možno považovať za záruku, neukladá sa ním však žiadna povinnosť, na základe ktorej by sa mali zaviesť záruky na zabezpečenie, že príjemca poskytne rovnakú úroveň ochrany, aká sa poskytuje zákonom o ochrane súkromných informácií. EDPB preto uznáva, že vo všeobecnosti sa použije informovaný súhlas dotknutej osoby ako základ pre prenosy údajov od prevádzkovateľov osobných informácií so sídlom v Kórei príjemcovi so sídlom v tretej krajine.

104. V tomto kontexte sú prínosom dodatočné objasnenia, ktoré poskytla Komisia pre ochranu osobných informácií v oznámení č. 2021-1, v súvislosti s povinnosťou informovať jednotlivcov o tretej krajine, do ktorej sa poskytnú ich údaje[43], keďže to pomôže dotknutým osobám v EHP urobiť plne informované rozhodnutie o tom, či vyjadria súhlas s poskytnutím údajov do zahraničia, ako to zdôraznila Európska komisia[44].

105. Ako sa konštatuje aj v stanovisku č. 28/2018 týkajúcom sa návrhu vykonávacieho rozhodnutia Európskej komisie o primeranej ochrane osobných údajov v Japonsku, musí sa však zdôrazniť, že podľa všeobecného nariadenia o ochrane údajov musia byť dotknuté osoby pred vyjadrením súhlasu výslovne informované o rizikách, ktoré takéto prenosy môžu predstavovať z dôvodu absencie primeranej ochrany v tretej krajine, ako aj absencie primeraných záruk. Takéto oznámenie by malo zahŕňať napríklad informáciu, že v tretej krajine nemusí existovať dozorný orgán a/alebo nemusia byť stanovené zásady spracúvania údajov a/alebo práva dotknutých osôb[45]. Podľa EDPB je poskytnutie týchto informácií nevyhnutné na to, aby sa dotknutej osobe s plnou znalosťou týchto konkrétnych skutočností týkajúcich sa prenosu umožnilo vyjadriť informovaný súhlas[46]. EDPB preto vyjadruje znepokojenie nad zisteniami Európskej komisie vo vzťahu k tomuto osobitnému druhu prenosov, ktoré uviedla v návrhu rozhodnutia o primeranosti. Dotknuté osoby obvykle nepoznajú rámec ochrany údajov v tretích krajinách. Nie je teda možné dospieť k záveru, že dotknutá osoba by dokázala posúdiť riziko, ktoré predstavuje prenos, len na základe znalosti konkrétnej krajiny určenia. Pred vyjadrením súhlasu dotknutej osoby je skôr potrebné poskytnúť jej jasné informácie o konkrétnych rizikách, ktoré takýto prenos osobných údajov do krajiny, ktorá sa nachádza mimo územia Kórejskej republiky, predstavuje.

106. EDPB teda vyzýva Európsku komisiu, aby zabezpečila, že informácie „*o okolnostiach sprevádzajúcich prenos*“, ktoré sa majú poskytnúť dotknutej osobe, zahŕňajú informácie o rizikách, ktoré prenosy môžu predstavovať z dôvodu absencie primeranej ochrany v tretej krajine, ako aj absencie primeraných záruk. Z pohľadu EDPB to je dôležité, aby mohol posúdiť, či sú požiadavky na vyjadrenie súhlasu v podstate rovnocenné s požiadavkami vo všeobecnom nariadení o ochrane údajov.

107. EDPB by vzhľadom na to, že súhlas musí byť slobodne daný, informovaný, konkrétny a jednoznačný, okrem toho uvítal, ak by rozhodnutie o primeranosti obsahovalo uistenia, že kórejskí prevádzkovatelia osobných informácií neprenesú osobné údaje tretej strane v tretej krajine za žiadnych okolností, keď nemožno podľa všeobecného nariadenia o ochrane údajov poskytnúť platný súhlas, napríklad v dôsledku nerovnováhy postavenia.

108. Pokiaľ ide o prípady, keď prevádzkovateľ osobných informácií môže poskytnúť osobné informácie tretej strane v zahraničí bez súhlasu dotknutej osoby – t. j. 1. ak sa osobné informácie poskytujú

[42] Odôvodnenie 88 návrhu rozhodnutia.
[43] Tamže.
[44] Tamže.
[45] Usmernenia EDPB č. 2/2018 o výnimkách podľa článku 49 nariadenia 2016/679 z 25. mája 2018, s. 8.
[46] Usmernenia EDPB č. 2/2018 o výnimkách podľa článku 49 nariadenia 2016/679 z 25. mája 2018, s. 7.

v rozsahu primerane súvisiacom s pôvodným účelom získavania podľa článku 17 ods. 4 zákona o ochrane osobných informácií; a 2. ak možno osobné informácie poskytnúť tretej strane vo výnimočných prípadoch uvedených v článku 18 ods. 2 zákona o ochrane osobných informácií – EDPB berie na vedomie vysvetlenia, ktoré poskytla Komisia pre ochranu osobných informácií v oddiele 2 oznámenia č. 2021-1 [a víta predpokladanú povinnosť uloženú prevádzkovateľovi so sídlom v Kórei a príjemcovi v zahraničí s cieľom zabezpečiť prostredníctvom právne záväzného nástroja (napr. zmluvou) úroveň ochrany, ktorá je rovnocenná úrovni poskytnutej zákonom o ochrane osobných informácií, a to aj v súvislosti s právami dotknutých osôb].

3.1.12. Priamy marketing

109. V súlade s článkami 21 ods. 2 a 3 GDPR a referenčným kritériom primeranosti podľa všeobecného nariadenia o ochrane údajov dotknutá osoba musí byť vždy schopná namietať proti spracúvaniu údajov na účely profilovania a priameho marketingu, a to bezplatne.

110. Pokiaľ ide o právo na pozastavenie spracúvania stanovené článkom 37 zákona o ochrane osobných informácií, EDPB uznáva, že Európska komisia skonštatovala, že toto právo sa vzťahuje aj na prípady, keď sa údaje používajú na účely priameho marketingu[47]. EDPB by však uvítal, keby boli v návrhu rozhodnutia uvedené dodatočné informácie a objasnenia v súvislosti s týmto posúdením, a najmä v súvislosti s uplatňovaním práva na pozastavenie spracúvania v kontexte priameho marketingu v praxi (napr. odkazy na príslušnú judikatúru atď.). V tejto súvislosti by EDPB navyše chcel zdôrazniť, že v zákone o používaní a ochrane úverových informácií (článok 37 ods. 2) je výslovne stanovené právo dotknutej osoby požiadať poskytovateľa/používateľa úverových informácií, aby ju prestali kontaktovať na účely predstavenia alebo ponúkania nákupu tovaru či služieb.

111. Okrem toho, ako uznáva Európska komisia[48], v kórejskom právnom rámci si takéto spracúvanie zvyčajne vyžaduje konkrétny (dodatočný) súhlas dotknutej osoby (pozri článok 15 ods. 1 pododsek 1, článok 17 ods. 2 pododsek 1 zákona o ochrane osobných informácií).

112. Keďže spracúvanie osobných údajov prenesených z EHP v Kórei na takéto účely nemožno vylúčiť, EDPB by takisto uvítal, ak by rozhodnutie o primeranosti obsahovalo objasnenia v súvislosti s existenciou práva dotknutej osoby odvolať súhlas[49] a práva na to, aby jej osobné údaje boli vymazané a prestali sa spracúvať, ak je spracúvanie založené na súhlase (ako je to v prípade spracúvania na účely marketingu) a dotknutá osoba súhlas odvolala.

3.1.13. Automatizované rozhodovanie a profilovanie

113. Ako Európska komisia konštatuje vo svojom návrhu rozhodnutia[50], zákon o ochrane osobných informácií a vykonávací dekrét k nemu neobsahujú všeobecné ustanovenia zamerané na problematiku rozhodnutí, ktoré majú vplyv na dotknutú osobu a sú založené výlučne na automatizovanom spracúvaní osobných údajov. V kórejskom právnom systéme sa predsa len s takýmto právom počíta v zákone o používaní a ochrane úverových informácií, ktorý obsahuje pravidlá týkajúce sa automatizovaných rozhodnutí (článok 36 ods. 2), a to aj keď sa zdá, že ich uplatňovanie nepatrí do rozsahu pôsobnosti dozoru Komisie pre ochranu informácií (a ako také do

[47] Odôvodnenie 79 návrhu rozhodnutia.
[48] Tamže.
[49] Pozri aj uvedený bod 67: Zatiaľ čo možnosť odvolať súhlas je jednoznačne stanovená v článku 37 ods. 1 zákona o používaní a ochrane úverových informácií, toto právo sa v zákone o ochrane osobných informácií spomína dvakrát, a to len v prípade osobitných okolností uvedených v článku 27 ods. 1 pododseku 2 a článku 39-7.
[50] Pozri odôvodnenie 81 návrhu rozhodnutia.

rozsahu pôsobnosti tohto návrhu rozhodnutia – pozri oddiel 2.3.2 o rozsahu uplatňovania návrhu rozhodnutia).

114. Ako už skonštatovala pracovná skupina zriadená podľa článku 29[51] vo svojom stanovisku 1/2016 o Privacy Shield a EDPB v predchádzajúcom stanovisku k rozhodnutiu o primeranosti, ktoré sa týkalo Japonska[52], čoraz väčší význam automatizovaného rozhodovania, profilovania a umelej inteligencie naznačuje, že by sa v tejto súvislosti mal prijať prístup, ktorý by zaručoval vyššiu ochranu. Na rozdiel od argumentov Európskej komisie, podľa ktorých je nepravdepodobné, že neexistencia osobitných pravidiel týkajúcich sa automatizovaného rozhodovania v zákone o ochrane osobných informácií[53] ovplyvní úroveň ochrany osobných údajov, ktoré boli získané v Únii (keďže každé rozhodnutie založené na automatizovanom spracúvaní by za normálnych okolností prijal prevádzkovateľ v Únii, ktorý má priamy vzťah s príslušnou dotknutou osobou), sa EDPB domnieva, že nemožno vylúčiť, že prevádzkovateľ osobných informácií so sídlom v Kórei by mohol využiť automatizované rozhodovanie v prípade údajov prenášaných na základe rozhodnutia o primeranosti (napríklad v kontexte zamestnanosti na posúdenie pracovnej výkonnosti, spoľahlivosti, správania atď.).

115. Vývoj nových technológií spoločnostiam umožňuje jednoduchšie zavádzanie alebo zvážiť zavádzanie systémov automatizovaného rozhodovania, v dôsledku ktorých sa môže oslabiť pozícia jednotlivcov. Ak rozhodnutia prijaté výlučne danými automatizovanými systémami ovplyvnia právne postavenie jednotlivcov alebo sa ich značne dotknú (napríklad zaradením na čiernu listinu, a teda odňatím práv jednotlivcov), je nevyhnutné poskytnúť dostatočné záruky vrátane práva byť informovaný o konkrétnych dôvodoch, ktoré sú základom rozhodnutia, a o vykonanom postupe, práva opraviť nesprávne alebo neúplné informácie a práva napadnúť rozhodnutie, ak bolo prijaté na nesprávnom vecnom základe.[54]

116. V tomto kontexte EDPB vyjadruje znepokojenie nad neexistenciou právnych ustanovení týkajúcich sa automatizovaného rozhodovania v zákone o ochrane osobných informácií, a preto vyzýva Európsku komisiu, aby sa na tento problém zamerala a v tejto súvislosti ďalej monitorovala vývoj kórejského legislatívneho rámca.

3.1.14. Zodpovednosť

117. V kórejskom právnom rámci je zahrnutých niekoľko pravidiel zameraných na zabezpečenie, že prevádzkovatelia osobných informácií zavedú primerané technické a organizačné opatrenia v záujme účinného dodržiavania svojich povinností v oblasti ochrany údajov a s cieľom byť schopný takéto dodržiavanie preukázať, a to aj príslušnému dozornému orgánu. EDPB konkrétne víta existenciu pravidiel na prijatie vnútorného plánu riadenia (článok 29 zákona o ochrane osobných informácií), povinnosť vykonávať tzv. posúdenie vplyvu na ochranu súkromia v prípadoch, keď spracúvanie predstavuje vyššie riziko možného porušenia ochrany súkromia (článok 33 ods. 1 uvedeného zákona a článok 35 vykonávacieho dekrétu k zákonu o ochrane osobných informácií), pravidlá odbornej prípravy personálu a dozoru nad ním (článok 28 uvedeného zákona), ako aj povinnosť určiť zodpovednú osobu pre ochranu súkromia (článok 31 uvedeného zákona v spojení s článkom 32 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

118. Pokiaľ ide o v podstate rovnocennú úroveň, ktorú zabezpečujú, EDPB súhlasí s názorom Európskej komisie – dokonca aj v prípadoch, keď sa zdá, že pravidlá sa pomerne odchyľujú od pravidiel

[51] Táto pracovná skupina bola zriadená podľa článku 29 smernice 95/46/ES. Bol to nezávislý európsky poradný orgán pre ochranu údajov a súkromia. Jej úlohy sú opísané v článku 30 smernice 95/46/ES a v článku 15 smernice 2002/58/ES. Pracovnou skupinou zriadenou podľa článku 29 je teraz EDPB.

[52] Stanovisko č. 28/2018 týkajúce sa návrhu vykonávacieho rozhodnutia Európskej komisie o primeranej ochrane osobných údajov v Japonsku z 5. decembra 2018.

[53] Odôvodnenie 81 návrhu rozhodnutia.

[54] WP 254, s. 7.

uvedených vo všeobecnom nariadení o ochrane údajov, napr. neexistuje ustanovenie, v ktorom sa uvádza potreba, aby bola zodpovedná osoba nezávislá, no jednoznačne sa stanovuje, že zodpovedná osoba podlieha vedeniu prevádzkovateľa osobných informácií (článok 31 ods. 4 zákona o ochrane osobných informácií) a nesmie byť neopodstatnene znevýhodnená v dôsledku vykonávania týchto funkcií (článok 31 ods. 5 zákona o ochrane osobných informácií) – a navrhol by Európskej komisii, aby pri preskúmaní rozhodnutia o primeranosti monitorovala skutočné uplatňovanie týchto ustanovení s cieľom posúdiť ich účinné vykonávanie.

3.2. Procesné mechanizmy a mechanizmy presadzovania práva

119. EDPB na základe kritérií stanovených v referenčnom kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov analyzoval tieto aspekty kórejského rámca ochrany údajov, ako sa uvádza v návrhu rozhodnutia: existencia a účinné pôsobenie nezávislého dozorného orgánu; existencia systému zabezpečujúceho dobrú úroveň súladu a systému prístupu k vhodným mechanizmom nápravy, ktorý umožní jednotlivcom v EHP disponovať prostriedkami na vykonávanie ich práv a snažiť sa o nápravu bez toho, aby sa stretli so zdĺhavými prekážkami pri správnej a súdnej náprave.

120. V súlade s kapitolou VI všeobecného nariadenia o ochrane údajov a kapitolou 3 referenčného kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov musí existovať jeden alebo viacero nezávislých dozorných orgánov, ktoré sú poverené monitorovaním, zabezpečovaním a presadzovaním dodržiavania súladu s ustanoveniami týkajúcimi sa ochrany údajov a súkromia v tretej krajine, s cieľom zaručiť rovnocennú úroveň ochrany ako v EHP.

121. Dozorný orgán musí v tejto súvislosti konať úplne nezávisle a nestranne pri plnení svojich úloh a výkone svojich právomocí, pričom nesmie požadovať ani prijímať žiadne pokyny. Okrem toho by dozorný orgán mal mať všetky potrebné a dostupné právomoci a úlohy, aby zabezpečil súlad s právami na ochranu údajov a zvyšoval povedomie. Mal by sa zvážiť aj personál a rozpočet dozorného orgánu. Dozorný orgán je takisto schopný začať konanie z vlastnej iniciatívy.

3.2.1. Príslušný nezávislý dozorný orgán

122. V Kórejskej republike je za monitorovanie a presadzovanie zákona o ochrane osobných informácií zodpovedná Komisia pre ochranu osobných informácií. Komisiu pre ochranu osobných informácií tvorí jeden predseda, jeden podpredseda a sedem komisárov. Predsedu a podpredsedu vymenúva prezident na odporúčanie premiéra. Pokiaľ ide o komisárov, dvaja sú vymenovaní na odporúčanie predsedu, dvaja na odporúčanie zástupcov politickej strany, do ktorej patrí prezident, a zvyšní traja členovia sú vymenovaní na odporúčanie zástupcov iných politických strán (článok 7-2 ods. 2 zákona o ochrane osobných informácií). Komisii pre ochranu osobných informácií pomáha sekretariát (článok 7-13) a môže vytvoriť podkomisie (zložené z troch komisárov), ktoré sa budú venovať menej závažným porušeniam a opakovaným problémom (článok 7-12 zákona o ochrane osobných informácií).

123. EDPB v tomto zmysle uznáva, že Komisia pre ochranu osobných informácií napriek svojej nedávnej reorganizácii, ktorá značne zmenila jej postavenie a právomoci, vložila výrazné úsilie do vybudovania požadovanej infraštruktúry, aby ju prispôsobila vykonávaniu zákona o ochrane osobných informácií a jeho najnovších zmien. V rámci tohto úsilia možno poukázať na zavedenie pravidiel Komisie pre ochranu osobných informácií, vypracovanie usmernení s cieľom poskytnúť pokyny k výkladu zákona o ochrane osobných informácií a zriadenie linky pomoci na poskytovanie poradenstva prevádzkovateľom podnikov a jednotlivcom v oblasti právnych predpisov týkajúcich sa ochrany údajov, ako aj mediačných služieb na vybavovanie sťažností. Medzi úlohy Komisie pre ochranu osobných informácií konkrétne patrí poskytovanie poradenstva v oblasti právnej úpravy a právnych predpisov týkajúcich sa ochrany údajov, vypracúvanie politík a usmernení v oblasti ochrany údajov, vyšetrovanie porušení individuálnych práv, vybavovanie sťažností a mediácia sporov, presadzovanie dodržiavania súladu so zákonom o ochrane osobných informácií, zabezpečovanie vzdelávania a šírenia

povedomia v oblasti ochrany údajov, ako aj výmena a spolupráca s orgánmi tretích krajín pre ochranu údajov[55].

124. Vymenovanie a zloženie Komisie pre ochranu osobných informácií je stanovené v článku 7-2 zákona o ochrane osobných informácií. Hoci nad Komisiou pre ochranu osobných informácií má právomoc premiér (a predsedu a podpredsedu vymenúva prezident na odporúčanie premiéra), v právnom rámci sa stanovuje, že komisári plnia svoje úlohy nezávisle podľa príslušnej právnej úpravy a svojho svedomia. EDPB uznáva inštitucionálne a procesné záruky uvedené v zákone o ochrane osobných informácií, predovšetkým v článkoch 7-4 až 7-7. EDPB by predsa len uvítal, ak by Európska komisia monitorovala akýkoľvek vývoj, ktorý by mohol ovplyvniť nezávislosť členov juhokórejského dozorného orgánu.

125. Navyše návrh rozhodnutia ešte nezahŕňa analýzu rozpočtu Komisie pre ochranu osobných informácií vrátane zdrojov financovania a transparentnosti rozpočtu. EDPB sa domnieva, že tento prvok, ktorý sa uvádza v článku 56 ods. 1 všeobecného nariadenia o ochrane údajov aj v procesných zásadách a mechanizmoch a zásadách a mechanizmoch presadzovania práva v súvislosti s ochranou údajov, na ktoré sa má prihliadať podľa referenčného kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov pri hodnotení systému krajiny alebo medzinárodnej organizácie, sa musí dôkladne zohľadniť, keďže ide o ukazovateľ hospodárskych a ľudských zdrojov, ktoré má dozorný orgán k dispozícii na nezávislé plnenie svojich zákonných povinností a úloh týkajúcich sa ochrany údajov, a preto by odporučil Európskej komisii, aby mu v návrhu rozhodnutia venovala viac priestoru.

3.2.2. Existencia systému ochrany údajov zabezpečujúceho dobrú úroveň súladu

126. Pokiaľ ide o presadzovanie práva, EDPB uznáva rozsah právomocí a sankcií Komisie pre ochranu osobných informácií v tejto oblasti, ako sa stanovujú v zákone o ochrane osobných informácií a zákone o používaní a ochrane úverových informácií, pričom berie na vedomie objasnenia uvedené v oznámení č. 2021-1, v súlade s ktorým sa podmienky uvedené v článku 64 ods. 1 zákona o ochrane osobných informácií a článku 45 ods. 4 zákona o používaní a ochrane úverových informácií[56] budú uplatňovať vždy, keď sa poruší niektorá zo zásad, z práv alebo povinností zahrnutých v právnej úprave na ochranu osobných informácií. Európskej komisii by však odporučil, aby dôkladne monitorovala uplatňovanie právomocí Komisie pre ochranu osobných informácií v praxi, aby mohla porušiteľovi nariadiť prijať opatrenia, ktoré považuje za primerané na základe článku 64 ods. 1 zákona o ochrane osobných informácií alebo článku 45 ods. 4 zákona o používaní a ochrane úverových informácií.

127. Ďalej má Komisia pre ochranu osobných informácií v súvislosti s nápravnými opatreniami stanovenými v článku 64 ods. 1 zákona o ochrane osobných informácií v prípade nedodržania nápravného opatrenia právomoc uložiť pokutu v maximálnej výške 50 miliónov kórejských wonov (článok 75 ods. 2 pododsek 13 zákona o ochrane osobných informácií). Táto suma zodpovedá hodnote 36 564 EUR. EDPB sa domnieva a vyjadruje znepokojenie, že takéto obmedzenie výšky peňažných sankcií nemusí mať dostatočne silný odrádzajúci vplyv na porušovateľov, aký sa predpokladá v zákone, aby sa zabezpečilo presadzovanie pravidiel ochrany údajov, keďže jeho výška sa nejaví primerane dostatočná na odradenie, predovšetkým v prípade veľkých organizácií či podnikov s rozsiahlymi finančnými prostriedkami.

128. Pokiaľ ide o možnosť, že Komisia pre ochranu osobných informácií môže vyžadovať, aby vedúci ústredného správneho orgánu vyšetril prevádzkovateľa osobných informácií alebo sa podieľal na vyšetrovaní porušení zákona o ochrane osobných informácií či dokonca v rámci svojej právomoci nariadil prevádzkovateľom osobných informácií nápravné opatrenia (článok 63 ods. 4 až 5 zákona

[55] Úlohy a právomoci Komisie pre ochranu osobných informácií sú stanovené najmä v článkoch 7-8 a 7-9, ako aj v článkoch 61 až 66 zákona o ochrane osobných informácií.

[56] T. j. *„usudzovanie, že porušením zákona sa pravdepodobne porušia práva a sloboda jednotlivcov v oblasti ochrany osobných informácií, a neprijatie opatrení pravdepodobne spôsobí škodu, ktorú bude ťažké napraviť“*.

o ochrane osobných informácií), EDPB konštatuje, že hoci sú nejaké informácie uvedené v odôvodnení 122 návrhu rozhodnutia, celkovo je povaha týchto iných orgánov a ich právne vzťahy s Komisiou pre ochranu osobných informácií skôr nejasná. Navyše v článku 68 ods. 1 zákona o ochrane osobných informácií sa odkazuje na množstvo subjektov, na ktoré by bolo možné delegovať právomoci Komisie pre ochranu osobných informácií. Aj keď sa zdá, že toto ustanovenie sa uplatňovalo len v súvislosti s Kórejskou agentúrou pre internet a bezpečnosť [Korean Internet and Security Agency][57], EDPB by uvítal objasnenia, pokiaľ ide o povahu možných interakcií medzi týmito subjektmi, a dôkladné monitorovanie uplatňovania tohto ustanovenia v budúcnosti s cieľom zabezpečiť nezávislosť subjektov poverených uplatňovaním pravidiel ochrany údajov.

129. Pokiaľ ide o sankcie, zdá sa, že v kórejskom systéme sa kombinujú rôzne druhy sankcií, od nápravných opatrení a správnych pokút po trestnoprávne sankcie, ktoré s pravdepodobnosťou môžu mať odrádzajúci vplyv, pričom kórejské orgány predstavili niekoľko príkladov pokút, ktoré v poslednom čase uložila Komisia pre ochranu osobných informácií, a to aj pokutu vo výške 6,7 miliardy kórejských wonov uloženú v decembri 2020 spoločnosti za porušenie rozličných ustanovení zákona o ochrane osobných informácií, ako aj ďalšiu pokutu vo výške 103,3 milióna kórejských wonov z 28. apríla 2021 uloženú spoločnosti pôsobiacej v oblasti technológie umelej inteligencie za porušenie pravidiel zákonnosti spracúvania, konkrétne súhlasu, a spracúvanie pseudonymizovaných informácií.

130. Hoci uvedené sumy môžu mať odrádzajúci vplyv, EDPB by uvítal dodatočné informácie o spôsobe, ktorý Komisia pre ochranu osobných informácií používa na výpočet výšky správnych pokút, napríklad pokút za nedodržanie nápravného opatrenia uložených v súlade s článkom 64 ods. 1 zákona o ochrane osobných informácií (pozri článok 75 ods. 2 pododsek 13 zákona o ochrane osobných informácií). Toto je relevantné najmä z hľadiska trestnoprávnych sankcií a uplatňovania (kórejského) zákona o trestnom konaní.

3.2.3. Systém ochrany údajov musí poskytovať podporu a pomoc dotknutým osobám pri uplatňovaní svojich práv a vhodné mechanizmy nápravy

131. Zdá sa, že kórejský systém v súvislosti s nápravou ponúka viacero možností, ako zabezpečiť primeranú úroveň ochrany, najmä presadzovanie individuálnych práv vďaka účinným správnym a súdnym prostriedkom nápravy vrátane náhrady škody.

132. Ako sa uvádza v odôvodneniach 132 a 133 návrhu rozhodnutia, kórejský systém okrem možností správnej a súdnej nápravy ponúka aj alternatívne mechanizmy, pomocou ktorých jednotlivci môžu vymôcť nápravu, a to call centrum pre ochranu súkromia, resp. Výbor pre mediáciu sporov [Dispute Mediaton Committe]. Keďže ide o dodatočné možnosti nápravy, EDPB by uvítal podrobnejšie vysvetlenie toho, ako dopĺňajú možnosti nápravy, ktoré môžu pred Komisiou pre ochranu osobných informácií a súdmi vymáhať dotknuté osoby, ktorých osobné údaje sa prenášajú do Kórey na základe rozhodnutia o primeranosti.

4. PRÍSTUP K OSOBNÝM ÚDAJOM PRENÁŠANÝM Z EURÓPSKEJ ÚNIE ORGÁNMI VEREJNEJ MOCI V JUŽNEJ KÓREI A ICH POUŽÍVANIE TÝMITO ORGÁNMI

133. Pokiaľ ide o posúdenie úrovne ochrany v oblasti presadzovania práva a národnej bezpečnosti, Európska komisia vo svojom návrhu rozhodnutia a zverejnených prílohách poskytla komplexné

[57] Pozri odôvodnenie 117 návrhu rozhodnutia a článok 62 vykonávacieho dekrétu.

informácie. EDPB preto upúšťa od opakovania väčšiny skutkových zistení a posúdení v tomto stanovisku.

134. Európska komisia dospela k záveru, že úroveň ochrany údajov v uvedených oblastiach zodpovedá požiadavkám stanoveným judikatúrou SDEÚ, a preto ju možno považovať za v podstate rovnocennú s úrovňou ochrany Európskej únie.

135. EDPB by ešte chcel vo všeobecnosti zdôrazniť, že dokonca aj v prípadoch, keď sa pri údajoch prenášaných z EÚ do Južnej Kórey zdá alebo Európska komisia tvrdí, že je nepravdepodobné, že na ne bude mať vplyv príslušná kórejská právna úprava, by sa mala posúdiť primeranosť kórejskej úrovne ochrany údajov. Ich význam preukazuje aj skutočnosť, že sa na ne zamerala samotná Európska komisia vo svojom návrhu rozhodnutia.

4.1 Všeobecný rámec ochrany údajov v kontexte prístupu vlády

136. Pokiaľ ide o prístup orgánov verejnej moci k osobným údajom, je potrebné preskúmať rôzne kórejské zákony, aby sa dala posúdiť úroveň ochrany práva na súkromie a ochranu údajov. EDPB v prvom rade konštatuje, že zákon o ochrane osobných informácií, ktorý je kľúčovým právnym predpisom o ochrane údajov, má rozsiahlu uplatniteľnosť. Hoci je zákon o ochrane osobných informácií v plnej miere uplatniteľný v oblasti presadzovania práva, jeho uplatniteľnosť na spracúvanie údajov na účely národnej bezpečnosti je obmedzená. V súlade s článkom 58 ods. 1 pododsekom 2 zákona o ochrane osobných informácií sa kapitoly III až VII nevzťahujú na spracúvanie osobných údajov na účely národnej bezpečnosti, no kapitoly I, II, IX a X sa vzťahujú aj na túto oblasť. Základné zásady zákona o ochrane osobných informácií, ako aj základné záruky práv dotknutých osôb a ustanovenia o dozore, presadzovaní práva a prostriedkoch nápravy sa teda vzťahujú na prístup národných bezpečnostných orgánov k osobným údajom a ich používanie.

137. V ústave Južnej Kórey sú takisto zakotvené základné zásady ochrany údajov, konkrétne zásady zákonnosti, nevyhnutnosti a proporcionality. Tieto zásady sa vzťahujú aj na prístup juhokórejských orgánov verejnej moci k osobným údajom v oblasti presadzovania práva a národnej bezpečnosti[58].

138. V oblasti presadzovania práva môže získavať osobné údaje polícia, prokurátori, súdy a ďalšie orgány verejnej moci na základe osobitných právnych predpisov, t. j. zákona o trestnom konaní, zákona o ochrane súkromia komunikácie, zákona o telekomunikáciách a zákona o oznamovaní a používaní špecifikovaných informácií o finančných transakciách, ktoré sa vzťahujú na trestné stíhanie a predchádzanie praniu špinavých peňazí a financovanie terorizmu. V týchto osobitných zákonoch sa ďalej stanovujú obmedzenia, záruky a výnimky.

139. V oblasti národnej bezpečnosti môže získavať osobné údaje a zachytávať komunikáciu na základe zákona o Národnej spravodajskej službe a ďalších „zákonov o národnej bezpečnosti“[59] Národná spravodajská služba. EDPB chápe, že Národná spravodajská služba pri výkone svojich právomocí musí dodržiavať súlad s uvedenými právnymi ustanoveniami, ako aj so zákonom o ochrane osobných informácií.

140. EDPB žiada Komisiu, aby objasnila, či v Kórei okrem Národnej spravodajskej služby jestvujú iné orgány, ktoré zodpovedajú za oblasť národnej bezpečnosti, keďže podľa prílohy I oddielu 6 sa zdá, že Európska komisia uvádza Národnú spravodajskú službu ako príklad národného bezpečnostného orgánu.

[58] Pozri odôvodnenie 145 návrhu rozhodnutia.

[59] K zákonom o národnej bezpečnosti patrí napríklad zákon o ochrane súkromia komunikácie, zákon o boji proti terorizmu na ochranu občanov a verejnej bezpečnosti alebo zákon o telekomunikáciách.

4.2. Ochrana a záruky v súvislosti s údajmi potvrdzujúcimi komunikáciu v kontexte prístupu vlády na účely presadzovania práva

141. Na základe príslušnej právnej úpravy, zákona o ochrane súkromia komunikácie, orgány presadzovania práva môžu prijať dva druhy opatrení na získanie prístupu k informáciám o komunikácii. V zákone o ochrane súkromia komunikácie sa rozlišujú opatrenia na zachytenie komunikácie, ktoré sa vzťahujú na získavanie obsahu bežnej pošty aj priame zachytávanie obsahu telekomunikácie[60], a získavanie tzv. údajov potvrdzujúcich komunikáciu [communication confirmation data]. Údaje potvrdzujúce komunikáciu zahŕňajú dátum telekomunikácie, čas jej začatia a ukončenia, počet odchádzajúcich a prichádzajúcich hovorov, ako aj číslo účastníka na druhej strane, frekventovanosť využívania, logy týkajúce sa používania telekomunikačných služieb a informácie o polohe[61].

142. EDPB poznamenáva, že v prípade údajov potvrdzujúcich komunikáciu sa zdá, že sa na ne nevzťahujú rovnaké záruky ako na údaje získané pomocou opatrení na zachytenie komunikácie, t. j. údaje o obsahu. EDPB skutočne konštatuje, že pri získavaní údajov o obsahu sa uplatňuje viac záruk ako pri získavaní údajov potvrdzujúcich komunikáciu na účely presadzovania práva: Po prvé získavanie údajov potvrdzujúcich komunikáciu na rozdiel od získavania údajov o obsahu nie je obmedzené na vyšetrovanie určitých závažných trestných činov, ale možno ho uskutočniť, ak sa považuje za nevyhnutné na zorganizovanie „akéhokoľvek vyšetrovania či výkon akéhokoľvek trestu“ (článok 13 ods. 1 zákona o ochrane súkromia komunikácie). Po druhé získavanie údajov potvrdzujúcich komunikáciu nemá v zásade štruktúru poslednej možnosti a využíva sa, len ak je náročné predísť spáchaniu trestného činu, zatknutiu páchateľa trestnej činnosti či získať dôkazy iným spôsobom[62]. Údaje potvrdzujúce komunikáciu možno získať vždy, keď to prokurátor alebo príslušník justičnej polície „považuje za nevyhnutné“ na vyšetrenie trestného činu či výkon trestu. V tejto súvislosti však podľa článku 13 ods. 2 zákona o ochrane súkromia komunikácie existuje výnimka pre sledovanie údajov v reálnom čase a údaje potvrdzujúce komunikáciu týkajúce sa konkrétnej základňovej stanice. Po tretie orgány presadzovania práva získavajúce obsah komunikácie musia bezodkladne toto získavanie ukončiť, ak sa už prístup ku komunikácii nepovažuje za nevyhnutný[63]. Pokiaľ ide o údaje potvrdzujúce komunikáciu, prinajmenšom sa to výslovne nestanovuje v zákone o ochrane súkromia komunikácie ani vo vykonávacom dekrétu k nemu.

143. EDPB berie na vedomie, že získavanie údajov potvrdzujúcich komunikáciu sa môže uskutočňovať len na základe súdneho príkazu. Podľa zákona o ochrane súkromia komunikácie sa navyše vyžadujú podrobné informácie, ktoré sa majú uviesť pri uplatňovaní príkazu, ako aj v samotnom príkaze[64]. Takéto predchádzajúce súdne povolenie slúži na obmedzenie diskrečnej právomoci orgánov presadzovania práva pri uplatňovaní zákonov a na overenie, či v každom prípade existujú dostatočné dôvody na získavanie údajov potvrdzujúcich komunikáciu. EDPB takisto uznáva, že právo Kórejskej republiky podľa všetkého neobsahuje ustanovenia o všeobecnom a nerozlišujúcom uchovávaní údajov potvrdzujúcich komunikáciu. Prístup vlády k takýmto údajom sa teda vždy týka údajov, ktoré sa naďalej uchovávajú na účely účtovania a samotného poskytovania komunikačných služieb.

144. EDPB však zdôrazňuje, že SDEÚ spochybnil skutočnosť, že prevádzkové údaje sú menej citlivé v porovnaní s inými druhmi údajov, a to najmä v porovnaní s údajmi o obsahu[65]. Vzhľadom na to, že

[60] Článok 3 ods. 2, článok 2 ods.6 a 7 zákona o ochrane súkromia komunikácie.
[61] Článok 2 ods. 11 zákona o ochrane súkromia komunikácie.
[62] Ide o údaje o obsahu v súlade s článkom 3 ods. 2 a článkom 5 ods. 1 zákona o ochrane súkromia komunikácie.
[63] Článok 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
[64] Pozri odôvodnenie 156 návrhu rozhodnutia.
[65] Pozri SDEÚ, C-623/17, Privacy International, 6. októbra 2020, ECLI:EU:C:2020:790, bod 71: *„Zásah do práva zakotveného v článku 7 Charty, ktorý spôsobuje odovzdávanie údajov o prenose dát a polohe bezpečnostným a spravodajským službám, treba považovať za obzvlášť závažný najmä vzhľadom na citlivú povahu informácií,*

vo viacerých aspektoch sa údajom potvrdzujúcim komunikáciu poskytuje nižšia úroveň ochrany než údajom o obsahu, EDPB vyzýva Európsku komisiu, aby dôkladne monitorovala, či sa zárukami stanovenými v kórejskom práve určenými pre takúto kategóriu osobných údajov zabezpečuje v podstate rovnocenná úroveň ochrany, ako je úroveň ochrany zaručená v EÚ, predovšetkým pokiaľ ide o proporcionalitu a predvídateľnosť zákonov.

4.3. Prístup k informáciám o komunikácii zo strany kórejských orgánov verejnej moci na účely národnej bezpečnosti

145. Pokiaľ ide o právny rámec prístupu národných bezpečnostných orgánov k informáciám o komunikácii prenášaným z EHP do Kórey, EDPB sa zameral na dve problematické miesta, pričom obidve sa týkajú režimu prístupu ku komunikácii medzi cudzími štátnymi príslušníkmi, ktorá patrí do osobitného súboru prípadov použitia (pozri bod 29). Na uvedené prípady súvisiace s údajmi potvrdzujúcimi komunikáciu a údajmi o obsahu sa určité záruky, ktoré by boli za iných okolností platné, nevzťahujú. Inými slovami, v týchto osobitných situáciách sa v prípade týchto údajov neuplatňujú rovnaké záruky ako v prípade údajov o komunikácii, ak je do nej zapojený aspoň jeden kórejský štátny príslušník.

4.3.1. Neexistencia povinnosti informovať jednotlivcov o prístupe vlády ku komunikácii medzi cudzími štátnymi príslušníkmi

146. V prípade uvedeného scenára, t. j. keď žiadna zo strán zúčastňujúcich sa na komunikácii nie je kórejským štátnym príslušníkom, národné bezpečnostné orgány nie sú povinné informovať jednotlivcov o získavaní a spracúvaní ich údajov. EDPB uznáva, že tento problém sa týka len niektorých prípadov. V prvom rade, ako už bolo uvedené, vždy, keď je do komunikácie zapojený aspoň jeden kórejský štátny príslušník, požiadavky na informovanie vyplývajúce zo zákona o ochrane súkromia komunikácie sa vzťahujú na všetky strany zúčastňujúce sa na komunikácii bez ohľadu na ich štátnu príslušnosť[66]. V druhom rade získavanie osobných údajov pochádzajúcich z komunikácie, ktorá sa uskutočňuje výlučne medzi cudzími štátnymi príslušníkmi, podlieha osobitnému súboru prípadov použitia. Konkrétnejšie právo na prístup sa v takýchto prípadoch vzťahuje aj na komunikáciu: a) krajín s nepriateľským postojom ku Kórejskej republike; b) cudzích orgánov, skupín alebo štátnych príslušníkov podozrivých z protikórejskej činnosti[67] alebo c) členov skupín z Kórejského polostrova mimo suverenity Kórejskej republiky a ich zastrešujúcich skupín so sídlom v cudzích krajinách. Komunikácia medzi jednotlivcami z EÚ prenášaná z EHP do Kórey sa teda môže získavať len na účely národnej bezpečnosti, ak patria do jednej z troch uvedených kategórií[68]. EDPB na základe dodatočných vysvetlení Európskej komisie pochopil ako ďalší obmedzujúci faktor aj to, že príslušný právny rámec neobsahuje ustanovenia o zachytávaní údajov v tranzite mimo Kórey.

147. Význam neexistencie požiadavky na informovanie teda možno z hľadiska jej dôsledkov v praxi považovať za obmedzený. EDPB však zdôrazňuje význam (následného) informovania o prístupe vlády, najmä v súvislosti so zabezpečením účinných prostriedkov nápravy. SDEÚ dospel k záveru, že daná informácia je pre dotknuté osoby „*nevyhnutná na to, aby mohli vykonať svoje práva vyplývajúce z článkov 7 a 8 Charty, požiadať o prístup k ich osobným údajom, ktoré boli predmetom týchto*

ktoré môžu z týchto údajov vyplynúť, a najmä možnosť vytvoriť z nich profily dotknutých osôb, pričom takáto informácia je rovnako citlivá ako samotný obsah komunikácie. Navyše môže v povedomí dotknutých osôb vyvolať pocit, že ich súkromný život je predmetom neustáleho sledovania (pozri analogicky rozsudky z 8. apríla 2014, Digital Rights Ireland a i., C‑293/12 a C‑594/12, EU:C:2014:238, body 27 a 37, ako aj z 21. decembra 2016, Tele2, C‑203/15 a C‑698/15, EU:C:2016:970, body 99 a 100).“

[66] Pozri odôvodnenie 192 návrhu rozhodnutia.

[67] Pozri prílohu II, poznámku pod čiarou č. 244, kde sa uvádza, že pojem „protikórejské činnosti“ sú činnosťami ohrozujúcimi existenciu a bezpečnosť národa, demokratické usporiadanie štátu alebo prežitie a slobodu ľudí.

[68] Pozri odôvodnenie 187 návrhu rozhodnutia.

opatrení, a prípadne o ich opravu alebo odstránenie, ako aj podať v súlade s článkom 47 prvým odsekom Charty účinný opravný prostriedok na súde“[69]. Súčasťou prístupu vlády na účely národnej bezpečnosti sú mnohokrát opatrenia tajného sledovania, čo znamená, že ciele sledovania, teda dotknuté osoby, nevedia o spracúvaní svojich údajov. A preto *„dotknutá osoba má v zásade len minimálnu možnosť obrátiť sa na súdy, pokiaľ nie je informovaná o opatreniach prijatých bez jej vedomia, a teda môže napadnúť ich zákonnosť so spätnou účinnosťou, alebo alternatívne, pokiaľ sa akákoľvek osoba, ktorá má podozrenie, že jej komunikácia je alebo bola zachytávaná, môže obrátiť na súdy, takže právomoc súdov nezávisí od informovania dotknutej osoby, že došlo k zachytávaniu jej komunikácie*“[70]. V tejto súvislosti a v súlade s uvedeným EDPB veľakrát vyjadril znepokojenie nad účinnými prostriedkami nápravy v prípadoch sledovania. EDPB zdôrazňuje, že utajenie opatrení vlády nesmie viesť k tomu, že takéto opatrenia nemožno účinne napadnúť. V tomto kontexte treba vyhodnotiť, či neexistencia požiadavky na informovanie v prípade komunikácie medzi cudzími štátnymi príslušníkmi ovplyvňuje úroveň ochrany údajov posudzovanú v návrhu rozhodnutia, ako súčasť celkového posúdenia s osobitným zreteľom na mechanizmy dozoru a nápravy stanovené v kórejskom práve (pozri oddiely 4.7 a 4.8).

148. EDPB navyše v tomto kontexte poznamenáva, že v právnej úprave sa odkazuje na pomerne obsiahle pojmy, ako sú „protikórejské“ či „protinárodné činnosti“[71], a že je náročné predvídať, ako sa tieto pojmy vykladajú podľa kórejských zákonov. EDPB vyzýva Európsku komisiu, aby monitorovala, ako sa tieto pojmy rozvíjajú v kórejských zákonoch a či ich uplatniteľnosť v praxi spĺňa požiadavky proporcionality v súlade s právom EÚ.

4.3.2. Neexistencia predchádzajúceho nezávislého povolenia na získavanie informácií o komunikácii medzi cudzími štátnymi príslušníkmi

149. V prípadoch, keď sa osobné údaje EHP získané z komunikácie medzi cudzími štátnymi príslušníkmi (a na ktorú sa vzťahuje jeden z uvedených prípadov použitia) majú spracúvať v Kórei na účely národnej bezpečnosti, získavanie takýchto údajov nepodlieha predchádzajúcemu schváleniu nezávislým orgánom (ako je to v prípade komunikácie, keď je aspoň jedna z dotknutých osôb kórejským štátnym príslušníkom).[72]

150. Predovšetkým s prihliadnutím na nedávne rozhodnutia ESĽP vo veci „Big Brother Watch a i./Spojené kráľovstvo“ a vo veci „Centrum för Rättvisa/Švédsko“ EDPB konštatuje, že je nevyhnutné preskúmať, či to predstavuje zásadný nedostatok kórejského rámca ochrany údajov. V tejto súvislosti EDPB pripomína v súlade s aktualizovanými odporúčaniami o európskych základných zárukách pre opatrenia týkajúce sa sledovania[73], v ktorých sa zdôrazňuje, že na základe článku 6 ods. 3 Zmluvy o Európskej únii sa stanovuje, že základné práva zakotvené v Európskom dohovore o ľudských právach tvoria všeobecné zásady právneho poriadku EÚ, zatiaľ čo v judikatúre SDEÚ sa pripomína, že tento dohovor nepredstavuje, kým k nemu Európska únia nepristúpila, právny nástroj formálne začlenený

[69] SDEÚ, spojené veci C-511/18, C-512/18 a C-520/18, La Quadrature du Net a i., 6. októbra 2020, ECLI:EU:C:2020:791, bod 190.

[70] ESĽP, Big Brother Watch a i./Spojené kráľovstvo, 25. mája 2021, ECLI:CE:ECHR:2021:0525JUD005817013, bod 337 a Európsky súd pre ľudské práva, Roman Zakharov/Rusko, 4. decembra 2015, ECLI:CE:ECHR:2015:1204JUD004714306, bod 234.

[71] Európska komisia uviedla, že podľa vysvetlení kórejskej vlády ide o „činnosti ohrozujúce existenciu a bezpečnosť národa, demokratické usporiadanie štátu alebo prežitie a slobodu ľudí“, pozri aj poznámku pod čiarou č. 319 návrhu rozhodnutia o primeranosti.

[72] Pozri odôvodnenie 190 návrhu rozhodnutia.

[73] Pozri odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania, body 10, 11.

do právneho poriadku Únie[74]. Úroveň ochrany základných práv vyžadovaná článkom 45 všeobecného nariadenia o ochrane údajov sa teda musí určiť na základe ustanovení tohto nariadenia v spojení so základnými právami zakotvenými v Charte. To znamená, že podľa článku 52 ods. 3 Charty práva v nej obsiahnuté, ktoré zodpovedajú právam zaručeným Európskym dohovorom o ľudských právach, majú rovnaký význam a rozsah pôsobnosti ako práva stanovené v uvedenom dohovore. Z toho vyplýva, že sa musí zohľadniť judikatúra ESĽP týkajúca sa práv, s ktorými sa takisto počíta v Charte, ako minimálna prahová hodnota ochrany na výklad zodpovedajúcich práv v Charte, t. j. pokiaľ sa na základe výkladu Charty SDEÚ nestanoví vyššia úroveň ochrany[75].

151. EDPB poznamenáva, že hoci predchádzajúce (nezávislé) schválenie opatrení sledovania sa považuje za dôležitú záruku proti svojvoľnosti, takéto schválenie nemožno odvodiť z judikatúry SDEÚ ako úplne nevyhnutnú požiadavku proporcionality opatrení sledovania. ESĽP však teraz výslovne stanovil požiadavku na predchádzajúce nezávislé povolenie v prípade hromadného zachytávania[76]. Hoci sa to v návrhu rozhodnutia výslovne neuvádza, EDPB chápe, že právny rámec Kórejskej republiky neobsahuje ustanovenia o hromadnom zachytávaní, ale len o cielenom zachytávaní komunikácie[77]. Európska komisia potvrdila tento výklad.

152. Vzhľadom na tieto skutočnosti uvedené rozhodnutia ESĽP v súlade s judikatúrou SDEÚ[78] a predchádzajúcou judikatúrou ESĽP[79] opäť poukazujú na význam komplexného dozoru, ktorý vykonávajú nezávislé dozorné orgány. EDPB zdôrazňuje, že nezávislý dozor vo všetkých štádiách procesu, keď vláda získava prístup na účely presadzovania práva a národnej bezpečnosti, je dôležitou zárukou proti svojvoľným opatreniam sledovania, a teda na posúdenie primeranej úrovne ochrany údajov. Cieľom záruky nezávislosti dozorných orgánov v zmysle článku 8 ods. 3 Charty je zaručiť účinné a spoľahlivé monitorovanie dodržiavania pravidiel o ochrane jednotlivcov týkajúcich sa spracúvania osobných údajov. Platí to najmä v prípadoch, keď sa v dôsledku povahy tajného sledovania jednotlivcovi bráni požiadať o preskúmanie alebo priamo sa zúčastniť na konaní o preskúmaní pred vykonávaním opatrenia sledovania alebo počas neho.

153. Neexistenciu predchádzajúceho nezávislého schválenia nemožno samo osebe považovať za podstatný nedostatok kórejského práva v súvislosti s posúdením v postate rovnocennej úrovne ochrany údajov. Posúdenie primeranosti opäť závisí od všetkých okolností prípadu, predovšetkým účinnosti dozoru *ex post* a právneho prostriedku nápravy, ako sa stanovuje v právnom rámci Kórey (pozri ďalšie oddiely 4.7 a 4.8).

[74] Pozri SDEÚ, C-311/18, Data Protection Commissioner/Facebook Ireland Ltd a Maximillian Schrems, 16. júla 2020, ECLI:EU:C:2020:559 (ďalej len „Schrems II“), bod 98.

[75] Pozri SDEÚ, spojené veci C-511/18, C-512/18 a C-520/18, La Quadrature du Net a i., 6. októbra 2020, bod 124.

[76] Pozri ESĽP, Big Brother Watch a i./Spojené kráľovstvo, 25. mája 2021, ECLI:CE:ECHR:2021:0525JUD005817013, bod 351: „Hromadné zachytávanie by malo podliehať nezávislému povoleniu udelenému na začiatku zachytávania“, „hromadné zachytávanie by mal povoliť nezávislý orgán, t. j. orgán, ktorý je nezávislý od výkonnej moci“.

[77] Jedine príloha II oddiel 3.2 obsahuje výslovné vyhlásenie na účely národnej bezpečnosti, ak sa spresňuje, že obmedzenia a záruky *„ zabezpečujú obmedzenie získavania a spracúvania informácií len na rozsah potrebný na dosiahnutie legitímneho zámeru. Tým je vylúčené akékoľvek plošné a nerozlišujúce získavanie osobných informácií na účely národnej bezpečnosti*“.

[78] Pozri napríklad spojené veci SDEÚ C-203/15 a C-698/15, Tele2 Sverige AB a i., ECLI:EU:C:2016:970.

[79] Pozri napríklad ESĽP, Roman Zakharov/Rusko, 4. decembra 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

4.4. Dobrovoľné sprístupnenie

154. V súlade s článkom 83 ods. 3 zákona o telekomunikáciách môžu poskytovatelia telekomunikačných služieb dobrovoľne odovzdať tzv. údaje o účastníkoch[80] národným bezpečnostným orgánom a orgánom presadzovania práva, ak o to požiadajú. EDPB poznamenáva, že hoci prípady týkajúce sa osobných údajov prenášaných z EHP do Kórey budú s pravdepodobnosťou zriedkavé, aj tak je potrebné zanalyzovať ich na posúdenie úrovne ochrany údajov, ako sa uvádza v predchádzajúcom texte.

155. EDPB chápe, že v týchto prípadoch sa uplatňujú záruky ochrany údajov podľa zákona o ochrane osobných informácií a orgány verejnej moci, ako aj poskytovatelia telekomunikačných služieb musia splniť tieto požiadavky[81], a že obidva tieto subjekty môžu niesť zodpovednosť za porušenie práv a slobôd príslušných dotknutých osôb[82]. EDPB ďalej chápe, že od poskytovateľov telekomunikačných služieb sa nevyžaduje, aby takéto požiadavky splnili.

156. Pokiaľ ide o koncepciu získania prístupu k údajom o účastníkoch vnútroštátnymi orgánmi presadzovania práva, a to konkrétne aj na účely národnej bezpečnosti, prostredníctvom „dobrovoľného sprístupnenia“ telekomunikačnými operátormi, práva a slobody dotknutých osôb, obzvlášť právo na informácie, však môžu byť vystavené vyššiemu riziku.

157. Podľa článku 58 ods. 1 pododseku 2 zákona o ochrane osobných informácií sa ustanovenia v kapitolách III až VII nevzťahujú na žiadne požadované osobné informácie, ktoré sa majú poskytnúť na účely národnej bezpečnosti. V tejto súvislosti sa napríklad ustanovenia článku 18 (Obmedzenie používania a poskytovania osobných informácií mimo stanoveného účelu) a článku 20 (Oznámenie zdrojov atď. osobných informácií získaných od tretích strán) zákona o ochrane osobných informácií nevzťahujú na takéto žiadosti. V prípadoch, keď žiadosť podá národný bezpečnostný orgán, vyvstáva na jednej strane otázka, či článok 58 ods. 1 pododsek 2 zároveň bráni uplatňovať zákon o ochrane osobných informácií aj poskytovateľom telekomunikačných služieb. Na druhej strane sa objavuje otázka, či sa vylúčenie uplatňovania článku 20 zákona o ochrane osobných informácií v takýchto prípadoch vzťahuje aj na príslušné ustanovenie v oddiele 3 prílohy I [Oznamovanie údajov, ak osobné údaje neboli získané od dotknutej osoby (článok 20 zákona)]. Ak by tomu tak bolo a článok 58 ods. 1 pododsek 2 bol určený aj poskytovateľom telekomunikačných služieb, podľa dostupných informácií by hrozilo riziko, že by neexistovala právna povinnosť informovať dotknuté osoby o dobrovoľnom sprístupnení.

158. EDPB preto vyjadruje znepokojenie nad účinnosťou, a teda že požiadavky na informácie by sa mohli stať neúčinnými, čo by znamenalo, že pre dotknuté osoby by bolo oveľa náročnejšie uplatniť si práva na ochranu údajov, najmä právo na súdny prostriedok nápravy. EDPB v tejto súvislosti vyzýva Európsku komisiu, aby objasnila rozsah pôsobnosti príslušných ustanovení.

4.5. Ďalšie použitie informácií

159. Zásada obmedzenia účelu je ústrednou právnou požiadavkou ochrany údajov. Vyžaduje, aby sa osobné údaje získavali na konkrétne určené, výslovne uvedené a legitímne účely a ďalej sa nespracúvali spôsobom, ktorý nie je zlučiteľný s uvedenými účelmi. Okrem toho sa orgánom verejnej moci podľa práva EÚ povoľuje spracúvať osobné údaje na predchádzanie trestným činom, ich vyšetrovanie alebo stíhanie, a to aj vtedy, keď sa dané údaje pôvodne získali na iný účel, pokiaľ tieto

[80] Medzi súbory údajov, ktorých sa to týka, patrí: meno, evidenčné číslo obyvateľa, adresa a telefónne číslo používateľov, dátumy využívania služby alebo ukončenia využívania služieb, ako aj identifikačné kódy (používané na identifikovanie oprávneného používateľa počítačových systémov alebo komunikačných sietí).
[81] Pozri odôvodnenia 164 až 194 návrhu rozhodnutia.
[82] Pozri odôvodnenie 166 návrhu rozhodnutia.

orgány majú právny základ na spracúvanie takýchto údajov podľa príslušnej právnej úpravy a pokiaľ ďalšie spracúvanie nie je neprimerané[83].

160. EDPB v súlade s uvedenými skutočnosťami berie na vedomie, že kórejský rámec ochrany údajov poskytuje podobné záruky a obmedzenia, ako sú tie, ktoré sa poskytujú v rámci práva EÚ v súvislosti s ďalším použitím informácií získaných na účely presadzovania práva a národnej bezpečnosti, napr. článok 3 ods. 1 až 2 zákona o ochrane osobných informácií o zásade obmedzenia účelu.

4.6. Následné prenosy a výmena spravodajských informácií

161. V článku 44 všeobecného nariadenia o ochrane údajov sa stanovuje, že prenosy a následné prenosy osobných údajov sa uskutočňujú len vtedy, ak nie je ohrozená úroveň ochrany zaručená všeobecným nariadením o ochrane údajov. Úroveň ochrany poskytovanej osobným údajom prenášaným z EHP do Kórey sa preto nesmie ohroziť ďalším prenosom príjemcom v tretej krajine, t. j. následné prenosy by sa mali povoliť len vtedy, ak je zabezpečená nepretržitá úroveň ochrany, ktorá je v podstate rovnocenná s úrovňou ochrany poskytovanou podľa práva EÚ. Z tohto vyplýva, že pri posudzovaní toho, či tretia krajina zabezpečuje primeranú úroveň ochrany údajov, sa musí zohľadniť právny rámec krajiny pre následné prenosy. Táto skutočnosť je nesporná a je v súlade s názorom tak Európskej komisie[84], ako aj EDPB.

162. EDPB v tejto súvislosti poznamenáva, že ESĽP vo svojich nedávnych rozsudkoch vo veci „Big Brother Watch a i./Spojené kráľovstvo“ a vo veci „Centrum för Rättvisa/Švédsko“ poskytol usmernenie[85] týkajúce sa preventívnych opatrení ochrany údajov, ktoré sa majú dodržiavať v zmluvných štátoch pri poskytovaní osobných údajov ďalším stranám na účely presadzovania práva a národnej bezpečnosti v prípadoch hromadného získavania: „*V prvom rade musia byť okolnosti, za ktorých sa takýto prenos môže uskutočniť, jasne stanovené vo vnútroštátnej právnej úprave. Po druhé musí štát, ktorý údaje prenáša, zabezpečiť, že štát, ktorý údaje prijíma, má pri manipulácii s údajmi zavedené záruky, na základe ktorých možno predísť zneužitiu a neprimeraným zásahom. Štát, ktorý údaje prijíma, musí konkrétne zaručiť bezpečné uchovávanie materiálu a zamedziť jeho následnému sprístupneniu. […] Po tretie budú potrebné posilnené záruky, ak bude zjavné, že sa prenáša materiál vyžadujúci osobitnú dôvernosť, ako je napríklad dôverný žurnalistický materiál*.“[86]

163. ESĽP pri uplatňovaní týchto noriem vo veci „Centrum för Rättvisa/Švédsko“ skonštatoval, že neexistencia akejkoľvek výslovnej právnej požiadavky v režime zachytávania na posúdenie nevyhnutnosti a proporcionality výmeny spravodajských informácií a jej možný vplyv na právo na súkromie predstavuje porušenie článku 8 Európskeho dohovoru o ľudských právach. ESĽP kritizoval to, že v dôsledku miery všeobecnosti právnej úpravy by zachytený materiál mohol byť zaslaný do zahraničia vždy, keď sa v tejto súvislosti usúdi, že je to v národnom záujme bez ohľadu na to, či zahraničný príjemca poskytuje prijateľnú minimálnu úroveň záruk[87].

164. EDPB berie na vedomie, že právny rámec Južnej Kórey neumožňuje hromadné zachytávanie, no vzhľadom na uvedené závery judikatúry ESĽP sa domnieva, že okrem požiadaviek vyplývajúcich z práva EÚ podľa výkladu SDEÚ by sa mala zvážiť argumentácia ESĽP s ohľadom na posudzovanie toho, či právny rámec pre následné prenosy do tretej krajiny poskytuje primerané normy ochrany údajov.

---

[83] Pozri článok 4 ods. 2 smernice o presadzovaní práva.

[84] Pozri odôvodnenie 84 a nasl. návrhu rozhodnutia.

[85] Ďalej uvedené prvky sa stanovili vo veciach Big Brother Watch a Centrum för Rättvisa, ktoré sa týkajú režimov hromadného zachytávania. Požiadavka na predbežné opatrenia, ktoré sa majú prijať pri poskytovaní materiálu ďalším stranám, bola už súčasťou kritérií, ktoré vypracoval ESĽP v kontexte cieleného zachytávania, pričom ju tento súd bližšie nespresnil (pozri Big Brother Watch a i./Spojené kráľovstvo, body 335, 362).

[86] ESĽP, Big Brother Watch a i./Spojené kráľovstvo, 25. mája 2021, ECLI:CE:ECHR:2021:0525JUD005817013, bod 362.

[87] Pozri ESĽP, Centrum för Rättvisa/Švédsko, 25. mája 2021, ECLI:CE:ECHR:2021:0525JUD003525208, bod 326.

1.6.1. Príslušný právny rámec pre následné prenosy orgánmi presadzovania práva

165. Pokiaľ ide o následné prenosy príslušnými orgánmi na účely presadzovania práva, EDPB z vysvetlení Európskej komisie chápe, že sa na ne vzťahuje oddiel 2 prílohy I k návrhu rozhodnutia týkajúci sa obmedzenia následných prenosov, a to aj pri prenose, ktorý sa uskutočňuje na základe iného zákona než zákona o ochrane osobných informácií. Podľa tohto pravidla: *„Ak sa osobné informácie poskytnú tretej strane v zahraničí, nemusí sa na ne vzťahovať úroveň ochrany zaručená kórejským zákonom o ochrane osobných informácií, keďže jednotlivé krajiny majú rôzne systémy ochrany osobných informácií. Vzhľadom na to sa budú takéto prípady považovať za ‚prípady, v ktorých môže dôjsť k znevýhodneniu dotknutej osoby', ktoré sú uvedené v článku 17 ods. 4 zákona, alebo za ‚prípady, v ktorých je nespravodlivo poškodený záujem dotknutej osoby alebo tretej strany', ktoré sú uvedené v článku 18 ods. 2 zákona a v článku 14-2 vykonávacieho dekrétu k tomu istému zákonu. Prevádzkovateľ osobných informácií a tretia strana musia preto s cieľom splniť požiadavky týchto ustanovení výslovne zabezpečiť úroveň ochrany rovnocennú úrovni ochrany v zákone, a to vrátane záruky uvedenej v právne záväzných dokumentoch, akými sú zmluvy, že dotknutá osoba si bude môcť uplatniť svoje práva aj po prenose osobných informácií do zahraničia*[88]*."*

166. EDPB víta toto ustanovenie, ktorým sa za predpokladu primeranosti úrovne ochrany údajov v Kórei na tento účel zabezpečuje nepretržitosť úrovne ochrany, aká sa v zásade vzťahuje na následné prenosy podľa práva EÚ. Komisia potvrdila, že výklad EDPB, ktorý spočíva v tom, že oddiel prílohy I sa vzťahuje na všetky následné prenosy príslušnými orgánmi na účely presadzovania práva, je správny. EDPB však poukazuje na to, že sa musí zaistiť, že tento právny predpis stanovuje nepretržitú úroveň ochrany v praxi, keďže z hľadiska zmluvných záruk a povinností či podobných mechanizmov, ktoré sa môžu použiť na dosiahnutie takejto úrovne ochrany pri spracúvaní na účely presadzovania práva, môže existovať neistota. V tejto súvislosti treba dodatočne uviesť, že napríklad osobné údaje možno poskytnúť len relevantným príslušným orgánom v tretej krajine.

167. To, či sa na Finančnú spravodajskú jednotku Kórey vzťahuje návrh rozhodnutia, podlieha už požadovanému objasneniu, pričom EDPB poznamenáva, že v oficiálnych vyhláseniach k prístupu vlády[89] sa vysvetľuje, že podľa článku 8 ods. 1 zákona o oznamovaní a používaní špecifikovaných informácií o finančných transakciách môže komisár Finančnej spravodajskej jednotky Kórey poskytovať zahraničným finančným spravodajským službám špecifikované informácie o finančných transakciách, ak sa to považuje za nevyhnutné na dosiahnutie účelu uvedeného zákona[90]. V samotnom článku 8 zákona o oznamovaní a používaní špecifikovaných informácií o finančných transakciách sa nestanovuje povinnosť určiť, či zahraničná krajina poskytuje primerané záruky ochrany údajov, ani zabezpečiť, aby ich poskytovala. Príloha II v tejto súvislosti neodkazuje na nový oddiel prílohy I. EDPB preto vyzýva Európsku komisiu, aby objasnila vzájomný vzťah príslušného oddielu prílohy I o obmedzení následných prenosov a právneho základu pre následné prenosy podľa zákona o oznamovaní a používaní špecifikovaných informácií o finančných transakciách.

[88] Návrh rozhodnutia, príloha I, s. 7.

[89] Pozri návrh rozhodnutia, príloha II.

[90] Pozri návrh rozhodnutia, príloha II oddiel 2.2.3.2. Zatiaľ čo takáto výmena sa môže uskutočniť len pod podmienkou, že zahraničná služba nebude môcť tieto informácie použiť na žiadny iný účel ako pôvodný účel ich sprístupnenia, a najmä nie na vyšetrovanie trestnej činnosti alebo na vedenie procesu (článok 8 ods. 2 zákona o oznamovaní a používaní špecifikovaných informácií o finančných transakciách), komisár Finančnej spravodajskej jednotky Kórey môže na základe prijatia žiadosti od cudzej krajiny vyjadriť súhlas s použitím takýchto údajov na vyšetrovanie trestnej činnosti alebo na vedenie procesu vo veci trestného činu, ak s tým vopred súhlasil minister spravodlivosti (článok 8 ods. 3 zákona o oznamovaní a používaní špecifikovaných informácií o finančných transakciách).

4.6.2. Príslušný právny rámec pre následné prenosy na účely národnej bezpečnosti

168. Návrh rozhodnutia neobsahuje žiadne informácie o právnom rámci pre následné prenosy v oblasti národnej bezpečnosti. EDPB teda chápe, že oddiel 2 prílohy I sa na rozdiel od účelov presadzovania práva na následné prenosy na účely národnej bezpečnosti nevzťahuje. Články 17 a 18 zákona o ochrane osobných informácií, ktorými sa zaoberá predmetný oddiel prílohy I, sú súčasťou kapitoly III uvedeného zákona, ktorá sa zase nevzťahuje na spracúvanie osobných na účely národnej bezpečnosti (článok 58 ods. 1 zákona o ochrane osobných informácií).

169. EDPB však predpokladá, že Kórea možno bude potrebovať preniesť osobné údaje, resp. prenesie ich zahraničným spravodajským službám na účely národnej bezpečnosti, napríklad s cieľom spolupracovať v boji proti cezhraničným hrozbám pre národnú bezpečnosť, varovať zahraničné vlády pred takýmito hrozbami či požiadať ich o pomoc pri identifikácii takýchto hrozieb.

170. EDPB pochopil, že podľa názoru Európskej komisie sú následné prenosy v kórejskom práve dostatočne upravené zárukami vyplývajúcimi zo zastrešujúceho ústavného rámca, najmä zásadami nevyhnutnosti a proporcionality, ako aj základnými zásadami ochrany údajov upravenými v zákone o ochrane osobných informácií, ako je zákonnosť a spravodlivosť spracúvania, obmedzenie účelu, minimalizácia údajov, bezpečnosť a všeobecné povinnosti zabrániť zneužitiu a nesprávnemu použitiu osobných informácií.

171. EDPB pripúšťa a uznáva všeobecnú uplatniteľnosť týchto kľúčových zásad (ochrany údajov), zároveň však vyjadruje znepokojenie, že tieto záruky majú príliš všeobecnú povahu a v právnom základe konkrétne neodkazujú ani sa nezameriavajú na osobitné okolnosti a podmienky následných prenosov údajov z EHP prenesených na účely národnej bezpečnosti. Hoci tieto všeobecné a zastrešujúce zásady majú širokú uplatniteľnosť, EDPB spochybňuje, či by sa to dalo považovať za splnenie podmienok jasných a presných pravidiel a dostatočného zakotvenia účinných a vymožiteľných záruk. Predovšetkým ak vláda získava prístup a spracúva osobné údaje v tajnosti a závery, ktoré by bo bolo možné z údajov vyvodiť, sú obzvlášť závažné, zavedenie jasných a podrobných pravidiel je nevyhnutné. V právnej úprave by sa mal na zabezpečenie primeranej ochrany jednotlivca dostatočne jasne uvádzať rozsah pôsobnosti akejkoľvek diskrečnej právomoci, ktorá bola príslušným orgánom udelená, a spôsob jej výkonu. SDEÚ v rozhodnutí vo veci Schrems II pripomína, že právny základ, ktorým sa povoľuje zasiahnuť do základných práv, musí sám osebe vymedzovať rozsah obmedzenia výkonu dotknutého práva a obsahovať jasné a presné pravidlá upravujúce rozsah pôsobnosti a uplatniteľnosť predmetného opatrenia a ukladať minimálne záruky, aby splnil požiadavky na zásady nevyhnutnosti a proporcionality[91]. EDPB preto vyjadruje znepokojenie, že všeobecné zakotvenie takýchto záruk do právneho predpisu vyššej právnej sily bez toho, aby sa osobitne zaviedol napr. pojem „proporcionalita“ do príslušného právneho základu, nepostačuje.

172. Toto znepokojenie posilňuje uvedené rozhodnutie ESĽP, v ktorom súd skonštatoval, že všeobecné pravidlo, ktoré neobsahuje výslovnú požiadavku na posúdenie nevyhnutnosti a proporcionality či nezohľadňuje obavy v súvislosti s ochranou súkromia, nie je zlučiteľné s právom na súkromie podľa článku 8 Európskeho dohovoru o ľudských právach. EDPB v tejto súvislosti poznamenáva, že v predmetnej judikatúre (ako aj v kórejskom práve) existujú zastrešujúce zásady nevyhnutnosti a proporcionality (zaručené ústavou), napr. podľa Charty alebo na základe pristúpenia k Európskemu dohovoru o ľudských právach.

173. EDPB vyzýva Európsku komisiu, aby objasnila právny základ, konkrétne spôsob, akým majú spravodajské služby povinnosť zohľadniť obavy v súvislosti s ochranou súkromia a záruky ochrany údajov pred poskytnutím osobných údajov zahraničným partnerom na účely národnej bezpečnosti, rozsah tejto povinnosti a osobitné podmienky jej uplatňovania. Ak takáto povinnosť vyplýva priamo z ústavných zásad, Európska komisia by mala ďalej posúdiť požiadavky na presnosť a jasnosť príslušnej

[91] Pozri vec Schrems II, body 175 a 180.

právnej úpravy a potvrdiť, že všeobecné ústavné záruky a záruky ochrany údajov sa primerane uplatňujú a vykonávajú.

4.6.3. Medzinárodné dohody

174. EDPB konštatuje, že Európska komisia vo svojom posúdení primeranosti nezohľadnila, či sú medzi Kóreou a tretími krajinami alebo medzinárodnými organizáciami uzavreté medzinárodné dohody, ktoré môžu obsahovať osobitné ustanovenia týkajúce sa medzinárodného prenosu osobných údajov orgánmi presadzovania práva a/alebo spravodajskými službami do tretích krajín. EDPB sa domnieva, že uzavretie dvojstranných a viacstranných dohôd s tretími krajinami na účely presadzovania práva alebo spravodajskej spolupráce s pravdepodobnosťou môže ovplyvniť posudzovanie kórejského právneho rámca ochrany údajov.

175. EDPB preto vyzýva Európsku komisiu, aby objasnila, či takéto dohody jestvujú, za akých podmienok ich možno uzavrieť, a posúdila, či ustanovenia medzinárodných dohôd môžu ovplyvniť úroveň ochrany, ktorá sa poskytuje osobným údajom prenášaným z EHP do Kórey na základe legislatívneho rámca, a postupy v súvislosti s poskytovaním údajov do zahraničia na účely presadzovania práva a národnej bezpečnosti.

4.7. Dozor

176. EDPB konštatuje, že dozor nad orgánmi presadzovania práva v trestných veciach, ako aj národnými bezpečnostnými orgánmi zabezpečuje kombinácia rôznych vnútorných a vonkajších orgánov.

177. V tejto súvislosti treba poznamenať, že SDEÚ opakovane zdôraznil potrebu nezávislého dozoru, ktorý je základným prvkom ochrany fyzických osôb, pokiaľ ide o spracúvanie ich osobných údajov. Pojem „nezávislosť“ zahŕňa oblasti inštitucionálnej autonómie, slobody z hľadiska pokynov a materiálnej nezávislosti. V záujme zabezpečenia konzistentného monitorovania a presadzovania právnych predpisov o ochrane údajov dozorné orgány musia mať účinné právomoci vrátane nápravných právomocí.

178. EDPB súhlasí so záverom Európskej komisie, že v celkovom posúdení možno skonštatovať, že Kórea má nezávislý a účinný systém dozoru, aj keď niektoré orgány v rámci tohto systému samy osebe nespĺňajú uvedené požiadavky. Napríklad väčšina z nich nemá výkonné právomoci, ale môžu prijímať len odporúčania, medzi ne patrí aj Národná komisia pre ľudské práva či Rada pre audit a inšpekciu. Okrem toho v prípade väčšiny príslušných orgánov verejnej moci nejde výhradne o inštitúcie na ochranu údajov, ale sú im zverené aj iné úlohy v oblasti ochrany základných práv.

179. EDPB však v súlade s vysvetleniami Európskej komisie konštatuje, že dozor nad orgánmi presadzovania práva zabezpečuje komplexným spôsobom a bez výnimky Komisia pre ochranu osobných informácií. Táto komisia má preto vyšetrovacie, nápravné právomoci a právomoci pre presadzovanie práva podľa zákona o ochrane osobných informácií a iných právnych predpisov o ochrane údajov (napr. zákona o ochrane súkromia komunikácie), ktoré sa vzťahujú na celú oblasť získavania prístupu k osobným údajom orgánmi presadzovania práva a národnými bezpečnostnými orgánmi.

180. V tomto kontexte by EDPB chcel opätovne zdôrazniť, že dozorné orgány musia mať dostatočné ľudské, technické a finančné zdroje, aby mohli vykonávať svoje úlohy a právomoci. V súvislosti s týmito zdrojmi nie je však, žiaľ, k dispozícii dostatok informácií o určených dozorných orgánoch, najmä o Komisii pre ochranu osobných informácií. Vzhľadom na to EDPB opakovanie žiada Európsku komisiu, aby na túto tému poskytla ďalšie informácie.

181. Celkovo by EDPB chcel poznamenať, že v návrhu rozhodnutia nie sú takmer žiadne vyjadrenia, príklady či číselné údaje týkajúce sa činností dozoru ani sa v ňom neuvádza presadzovanie právnych predpisov o ochrane údajov dozornými orgánmi v oblasti presadzovania práva a národnej bezpečnosti. Tieto informácie by boli užitočné v kontexte hodnotenia účinnosti dozorných orgánov.

1.8. Súdne prostriedky nápravy

182. EDPB pripomína, že na zabezpečenie primeranej úrovne ochrany údajov je nevyhnutné dotknutým osobám poskytnúť komplexné prostriedky nápravy proti neoprávnenému prístupu k údajom alebo ich neoprávnenému spracúvaniu. Tieto právne prostriedky nápravy musia byť dostatočné, aby dotknutá osoba mohla získať prístup k uchovávaným údajom o sebe a požiadať, aby sa jej údaje opravili alebo vymazali.

183. Vzhľadom na rozsudky SDEÚ vo veciach Schrems I a Schrems II je jasné, že okrem práva obrátiť sa na príslušné orgány má účinná súdna ochrana v zmysle článku 47 ods. 1 Charty zásadný význam z hľadiska predpokladu primeranosti práva tretej krajiny.

184. EDPB uznáva, že Kórea stanovila viaceré možnosti uplatňovania individuálnych práv na prístup, uchovávanie, vymazanie a pozastavenie spracúvania podľa zákona o ochrane osobných informácií. Uvedené práva možno uplatniť voči samotnému prevádzkovateľovi alebo prostredníctvom sťažnosti, ktorá sa predkladá Komisii pre ochranu osobných informácií či iným dozorným orgánom, ako je Národná komisia pre ľudské práva. EDPB ďalej uznáva možnosť napadnúť rozhodnutie prevádzkovateľov alebo orgánov verejnej moci v reakcii na ich žiadosť na základe Správneho súdneho poriadku.

185. EDPB navyše podľa vysvetlení poskytnutých Európskou komisiou chápe, že jednotlivci môžu napadnúť konanie orgánov presadzovania práva alebo národných bezpečnostných orgánov pred príslušnými súdmi na základe Správneho súdneho poriadku a zákona o ústavnom súde a zároveň majú možnosť získať náhradu škody na základe zákona o štátnom odškodnení[92].

186. V tejto súvislosti však EDPB vyjadruje znepokojenie nad účinnými prostriedkami nápravy pre jednotlivcov v EÚ v prípadoch národnej bezpečnosti, ktoré nezahŕňajú kórejských občanov. Ako sa uvádza v bode 33 a nasl., od národných bezpečnostných orgánov sa nevyžaduje, aby dotknuté osoby informovali o získavaní a spracúvaní ich údajov. Keďže v týchto prípadoch je omnoho náročnejšie získať účinnú právnu ochranu, EDPB by chcel zdôrazniť, že ak sú súčasťou prenosu údaje z EHP, určité právne záruky musia byť podmienkou. Tieto záruky musia dotknutým osobám umožňovať prijímanie účinných opatrení proti nezákonnému spracúvaniu údajov spôsobom, ktorý je z právneho hľadiska bezpečný, bez toho, aby pre ne predstavovali prekážku neprimerane striktné procedurálne požiadavky, ako je uloženie dôkazného bremena, ktoré nemôžu splniť bez toho, aby o spracúvaní vedeli. Popritom dotknuté osoby musia byť schopné obrátiť sa na príslušný orgán, ktorý spĺňa požiadavky článku 47 Charty, t. j. orgán, ktorý má právomoc určiť, či sa údaje spracúvajú, overiť zákonnosť spracúvania a ktorý má vymožiteľné nápravné právomoci v prípade, že je spracúvanie údajov nezákonné. V tomto kontexte by samotné právo na podanie sťažnosti napríklad Národnej komisii pre ľudské práva nepostačovalo. EDPB preto vyzýva Komisiu, aby podrobnejšie vysvetlila spôsob, akým sa tieto podmienky zavádzajú do procedurálnych a hmotnoprávnych požiadaviek, ako je napríklad to, či sa dotknuté osoby môžu obrátiť na Komisiu pre ochranu osobných informácií, ako aj na súd bez toho, aby museli dokazovať predmetné spracúvanie údajov.

187. EDPB zároveň konštatuje, že v návrhu rozhodnutia sa počíta s mechanizmom postupovania sťažností, t. j. jednotlivci v EÚ môžu predložiť Komisii pre ochranu osobných informácií sťažnosť prostredníctvom svojho vnútroštátneho orgánu pre ochranu údajov alebo EDPB. Komisia pre ochranu osobných informácií po skončení vyšetrovania informuje jednotlivca rovnakým spôsobom[93]. EDPB víta úsilie poskytnúť jednoduchší prístup k prostriedkom nápravy proti kórejským národným bezpečnostným orgánom. EDPB takisto presadzuje, aby takýto mechanizmus postúpenia sprostredkúvali európske

[92] Pozri prílohu II, oddiel 3.2.4 v spojení s oddielom 2.4.3.
[93] Pozri odôvodnenie 205 a prílohu I, s. 19 návrhu rozhodnutia.

vnútroštátne orgány pre ochranu údajov, a nie EDPB, keďže tieto orgány majú právomoc vybavovať individuálne sťažnosti a sú k nim bližšie.

188. EDPB ďalej konštatuje, že v súvislosti s dobrovoľným sprístupnením sa vyskytuje možný rozpor. Na jednej strane sa v návrhu rozhodnutia uvádza, že jednotlivci môžu vymáhať nápravu, ak sa ich údaje poskytli nezákonným spôsobom, na základe žiadosti o dobrovoľné sprístupnenie, a to aj nápravu proti orgánu presadzovania práva, ktorý žiadosť vydal[94]. Na druhej strane sa v návrhu rozhodnutia odkazuje na požiadavku priameho vplyvu na právo jednotlivca napadnúť konanie orgánov verejnej moci, pričom sa ako príklad uvádzajú (len) záväzné žiadosti o sprístupnenie informácií v prípade domnienky, že konanie správneho orgánu malo priamy vplyv na právo na súkromie[95]. EDPB podľa vysvetlení poskytnutých Európskou komisiou chápe, že v skutočnosti neexistuje obmedzenie možností nápravy proti žiadostiam o dobrovoľné sprístupnenie informácií, a preto vyzýva Európsku komisiu, aby túto záležitosť bližšie objasnila vo svojom rozhodnutí, a to v oblasti presadzovania práva aj národnej bezpečnosti (v oddiele o dobrovoľnom sprístupnení na účely národnej bezpečnosti sa na rozdiel od oddielu o presadzovaní práva žiadnym spôsobom výslovne neuvádzajú prostriedky nápravy v tomto kontexte).

[94] Pozri odôvodnenie 166 návrhu rozhodnutia.

[95] Pozri odôvodnenie 181 (presadzovanie práva) a odôvodnenia 208 a 181 (národná bezpečnosť) návrhu rozhodnutia.