Stanovisko 32/2021 k návrhu prováděcího rozhodnutí Evropské komise na základě nařízení (EU) 2016/679 o odpovídající ochraně osobních údajů v Korejské republice

verze 1.0

Přijato dne 24. září 2021

OBSAH

Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. s) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „**GDPR**“),

s ohledem na Dohodu o Evropském hospodářském prostoru (dále jen „**EHP**“) a zejména na přílohu XI a protokol 37 k této dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[1],

s ohledem na články 12 a 22 svého jednacího řádu,

PŘIJAL TOTO STANOVISKO:

1. SHRNUTÍ

1. Evropská komise zahájila formální proces směřující k přijetí návrhu prováděcího rozhodnutí (dále jen „**návrh rozhodnutí**“) o přiměřené ochraně osobních údajů v Korejské republice podle zákona o ochraně osobních údajů podle GDPR dne 16. června 2021[2].

2. Ve stejný den požádala Evropská komise o stanovisko Evropský sbor pro ochranu osobních údajů (dále jen „**EDPB**“)[3]. EDPB posoudil přiměřenost úrovně ochrany poskytované v Korejské republice na základě přezkoumání samotného návrhu rozhodnutí a na základě analýzy dokumentace zpřístupněné[4] Evropskou komisí.

3. EDPB se zaměřil na posouzení obecných aspektů návrhu rozhodnutí i přístupu orgánů veřejné moci k osobním údajům předávaným z EHP pro účely prosazování práva a národní bezpečnosti, včetně právní ochrany dostupné fyzickým osobám z EHP. EDPB rovněž posoudil, zda jsou záruky poskytované na základě korejského právního rámce zavedeny a zda jsou účinné.

4. EDPB použil jako hlavní referenci pro tuto práci svůj referenční rámec pro odpovídající ochranu[5] (dále jen „**referenční rámec pro odpovídající ochranu“**) přijatý v únoru 2018 a doporučení EDPB 02/2020 týkající se evropských základních záruk pro sledovací opatření[6].

1.1. Oblasti sbližování

5. Klíčovým cílem EDPB je poskytnout Evropské komisi stanovisko k přiměřenosti úrovně ochrany poskytované jednotlivcům, jejichž osobní údaje jsou předávány do Korejské republiky. Je třeba si uvědomit, že EDPB neočekává, že korejský právní rámec pro ochranu osobních údajů bude kopírovat evropské právní předpisy v oblasti ochrany osobních údajů.

[1] Pokud se v tomto stanovisku hovoří o „**členských státech**”, rozumějí se tím „členské státy EHP“.
[2] Viz tisková zpráva https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Tamtéž.
[4] EDPB založil svou analýzu na oficiálních překladech vyhotovených korejskou vládou.
[5] WP254, Referenční rámec pro odpovídající ochranu, 6. února 2018 (schválený EDPB, viz https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Viz doporučení EDPB 02/2020 týkající se evropských základních záruk pro sledovací opatření, přijaté dne 10. listopadu 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

6. EDPB však připomíná, že aby bylo možné považovat poskytovanou úroveň ochrany za odpovídající, vyžadují článek 45 GDPR a judikatura Soudního dvora Evropské unie (dále jen „**SDEU**“), aby právní předpisy třetí země byly v souladu se základními zásadami zakotvenými v GDPR. V této souvislosti vykazuje korejský rámec pro ochranu osobních údajů mnoho podobností s evropským rámcem pro ochranu osobních údajů, přičemž má jeden hlavní právní předpis pokrývající veřejný i soukromý sektor, který je doplněn zákony specifickými pro různá odvětví.

7. Pokud jde o obsah, EDPB bere na vědomí klíčové oblasti souladu mezi GDPR a korejským rámcem pro ochranu osobních údajů s ohledem na některá klíčová ustanovení, například u konceptů (např. „osobní údaje“, „zpracování“, „subjekt údajů“); důvody pro zákonné a spravedlivé zpracování pro legitimní účely; omezení účelu; kvalita a přiměřenost údajů; uchovávání údajů, bezpečnost a důvěrnost; transparentnost a zvláštní kategorie údajů.

8. Kromě výše uvedeného EDPB vítá snahy Evropské komise a korejských orgánů zajistit, aby Korejská republika poskytovala úroveň ochrany odpovídající GDPR prostřednictvím přijímání oznámení korejským dozorovým úřadem (která se týkají nejen předávání osobních údajů z EHP do Koreje) s cílem překlenout mezery mezi GDPR a korejským rámcem pro ochranu osobních údajů. V této souvislosti si EDPB přeje zdůraznit význam těchto oznámení pro posouzení přiměřenosti Korejské republiky s tím, že například poskytují relevantní vysvětlení některých důležitých ochranných opatření, mimo jiné ve vztahu k oblasti působnosti výjimky ze zákona o ochraně osobních údajů (PIPA) ohledně zpracování pseudonymizovaných osobních údajů pro vědecké, výzkumné a statistické účely, další předávání údajů a pravidla platná v souvislosti s přístupem orgánů veřejné moci k osobním údajům.

1.2. Výzvy

9. Ačkoli EDPB označil mnoho aspektů korejského rámce pro ochranu osobních údajů za v zásadě rovnocenné evropskému rámci pro ochranu osobních údajů, dospěl rovněž k závěru, že existují určité aspekty, které mohou vyžadovat bližší pohled a vyjasnění. Konkrétně se EDPB domnívá, že by měly být dále posouzeny následující položky, aby byla zajištěna v zásadě rovnocenná úroveň ochrany, a že by tyto položky měly být Evropskou komisí pečlivě sledovány.

1.2.1. Obecně

10. EDPB bere na vědomí, že oznámení č. 2021-1 *má status správního pravidla s právně závaznou platností pro správce osobních údajů v tom smyslu, že jakékoli porušení tohoto oznámení může být považováno za porušení příslušných ustanovení zákona o ochraně osobních údajů (PIPA)*[7]. Vzhledem k tomu, že toto oznámení neobsahuje dodatečná pravidla jako taková, ale spíše upřesnění toho, jak by mělo být chápáno použití textu zákona o ochraně osobních údajů (PIPA), a ve světle jeho celkového významu zejména s ohledem na ustanovení o pseudonymizaci podle zákona o ochraně osobních údajů (PIPA), která jsou předmětem probíhajících soudních případů, EDPB Evropskou komisi vyzývá, aby poskytla další informace o závaznosti, vymahatelnosti a platnosti oznámení č. 2021-1, a doporučuje pozorné sledování jeho dodržování v praxi, zejména jeho uplatňování nejen korejským dozorovým úřadem, ale také soudy, především tam, kde rovnocenná úroveň ochrany poskytovaná korejským právní rámcem vychází z vyjasnění, která jsou v tomto oznámení uvedena.

1.2.2. Obecné aspekty ochrany údajů

11. Pokud jde o rozsah použití rozhodnutí o odpovídající ochraně, EDPB poznamenává, že se bude vztahovat na předávání údajů z právního rámce EHP jak veřejným, tak soukromým „správcům osobních údajů“ spadajícím do působnosti zákona o ochraně osobních údajů (PIPA). EDPB chápe, že do tohoto pojmu jsou zahrnuty subjekty jednající jako zpracovatelé ve smyslu GDPR, avšak aby se

[7] Viz oddíl I přílohy I návrhu rozhodnutí.

předešlo nedorozuměním, vyzývá Evropskou komisi, aby objasnila, že rozhodnutí o odpovídající ochraně bude zahrnovat i předávání údajů „zpracovatelům“ v Koreji.

12. Důležitý aspekt, na který by chtěl EDPB upozornit, se týká konceptu pseudonymizovaných informací v korejském rámci pro ochranu údajů. Podle korejského práva se na zpracování pseudonymizovaných osobních údajů vztahují výjimky z řady příslušných ustanovení, včetně ustanovení o právech jednotlivých subjektů údajů a uchovávání údajů. Podle Evropské komise toto platí jen v případě, že jsou pseudonymizované osobní údaje zpracovávány pro účely statistik, vědeckého výzkumu nebo archivace ve veřejném zájmu. Toto tvrzení je však podporováno zejména oznámením č. 2021-1, což v této souvislosti podtrhuje již zmíněnou potřebu dodatečných informací a monitorování závaznosti, vymahatelnosti a platnosti tohoto oznámení. Kromě toho EDPB navrhuje Evropské komisi, aby dále posoudila dopad pseudonymizace podle korejského práva a především to, jak může ovlivnit základní práva a svobody subjektů údajů, jejichž osobní údaje jsou předávány do Korejské republiky na základě rozhodnutí o odpovídající ochraně. EDPB zejména vyzývá Evropskou komisi, aby dále posoudila odchylky uvedené v čl. 28 odst. 7 zákona o ochraně osobních údajů (PIPA) a čl. 40 odst. 3 zákona o používání a ochraně úvěrových informací (CIA) a aby pozorně sledovala jejich používání a příslušnou judikaturu, aby bylo zajištěno, že subjekty údajů nebudou nepřiměřeně omezovány, pokud jsou pro tyto účely zpracovávány osobní údaje předávané na základě rozhodnutí o odpovídající ochraně.

13. EDPB dále podotýká, že podle korejského práva existuje právo odvolat souhlas pouze za zvláštních okolností, a proto vyzývá Evropskou komisi, aby dále posoudila dopad nedostatku obecného práva na odvolání souhlasu a poskytla další záruky, aby zajistila, že základní úroveň ochrany údajů bude vždy zaručena, je-li to potřeba, též vyjasněním úlohy práva na pozastavení podle zákona o ochraně osobních údajů (PIPA) v případě neexistence obecného práva na odvolání souhlasu.

14. Pokud jde o další předávání údajů, EDPB uznává, že informovaný souhlas subjektu údajů se obecně použije jako základ pro předávání údajů od korejského správce osobních údajů příjemci se sídlem ve třetí zemi, přičemž oznámení č. 2021-1 předpokládá, že jednotlivci musí být informováni o takové třetí zemi, které budou jejich údaje poskytnuty. EDPB však vyzývá Evropskou komisi, aby zajistila, že informace, které mají být poskytnuty subjektu údajů, budou rovněž zahrnovat informace o možných rizicích předávání údajů vyplývajících z neexistence odpovídající ochrany ve třetí zemi, jakož i z neexistence vhodných záruk. EDPB by navíc uvítal ujištění v rámci rozhodnutí o odpovídající ochraně, že osobní údaje nebudou předávány od korejských správců osobních údajů do třetí země v žádné situaci, v níž by podle GDPR nemohl být udělen platný souhlas, např. kvůli nerovnováze sil.

15. Pokud jde o jmenování členů korejského dozorového úřadu, ačkoli by byl formální postup v souladu s GDPR, a proto by splňoval test rovnocennosti s právním rámcem EHP, EDPB by uvítal, kdyby Evropská komise sledovala veškerý vývoj, který by mohl ovlivnit nezávislost členů jihokorejského dozorového úřadu.

16. Pokud jde o rozpočet, opět na základě informací poskytnutých Evropskou komisí, není uveden žádný odkaz na konkrétní charakteristiku zaměstnanců korejské komise pro ochranu osobních údajů (PIPC) ani na finanční zdroje, které má tato komise k dispozici. EDPB by proto uvítal v návrhu rozhodnutí další informace o těchto dvou podstatných tématech.

1.2.3. Přístup orgánů veřejné moci k údajům předávaným do Korejské republiky

17. EDPB rovněž analyzoval korejský právní rámec s ohledem na přístup vlády za účelem vymáhání práva a národní bezpečnosti k osobním údajům předávaným z EHP do Koreje. Ačkoli EDPB uznává prohlášení a záruky poskytnuté korejskou vládou, jak je uvedeno v příloze II návrhu rozhodnutí, EDPB identifikoval řadu aspektů, které vyžadují vyjasnění nebo vyvolávají obavy.

18. EDPB podotýká, že ustanovení zákona o ochraně osobních údajů (PIPA) platí bez omezení v oblasti vymáhání práva. EDPB rovněž konstatuje, že na zpracování údajů v oblasti národní bezpečnosti se vztahuje omezenější soubor ustanovení zakotvených v zákoně o ochraně osobních údajů (PIPA).

19. Pokud jde o dobrovolné sdělování osobních údajů ze strany poskytovatelů telekomunikačních služeb národním bezpečnostním orgánům, EDPB je znepokojen nejasným vztahem oddílu 3 přílohy I návrhu rozhodnutí, který stanoví, že poskytovatelé v zásadě musí informovat dotyčnou osobu, pokud dobrovolně vyhoví žádosti, k článku 58 odst. 1 bodem 2 zákona o ochraně osobních údajů (PIPA), tj. s částečnou výjimkou pro účely národní bezpečnosti. To by mohlo způsobit neúčinnost požadavků na informace, což by subjektům údajů značně ztěžovalo uplatnění práv na ochranu údajů, zejména pokud jde o soudní nápravu.

20. Ačkoli to návrh rozhodnutí výslovně neuvádí, EDPB z vysvětlení poskytnutých Evropskou komisí chápe, že korejský právní rámec neumožňuje hromadný odposlech údajů z telekomunikačních prostředků. Nedávná judikatura Evropského soudu pro lidská práva (dále jen „**ESLP**“) týkající se režimů hromadného odposlechu by proto pro hodnocení úrovně ochrany údajů v Koreji nebyla přímo relevantní.

21. Návrh rozhodnutí neobsahuje žádné informace o právním rámci pro další předávání údajů v oblasti národní bezpečnosti. Přestože EDPB chápe, že podle názoru Evropské komise je další předávání údajů pro účely národní bezpečnosti dostatečně regulováno obecnými zárukami a zásadami vyplývajícími z ústavního rámce a ze zákona o ochraně osobních údajů (PIPA), EDPB má pochyby, zda to lze považovat za splnění požadavků na přesnost a jasnost zákona a zda jsou tím zakotvena účinná a vymahatelná ochranná opatření. Záruky, na které se Evropská komise odvolává, jsou velmi obecné povahy a v právním základě neřeší konkrétní okolnosti a podmínky, za nichž může docházet k dalšímu předávání údajů pro účely národní bezpečnosti. V této souvislosti EDPB rovněž podotýká, že Evropská komise nezohlednila existenci mezinárodních dohod uzavřených mezi Korejskou republikou a třetími zeměmi nebo mezinárodními organizacemi, které by mohly obsahovat zvláštní ustanovení pro mezinárodní předávání osobních údajů donucovacími orgány nebo zpravodajskými službami do třetích zemí. EDPB se domnívá, že uzavření dvoustranných nebo mnohostranných dohod se třetími zeměmi za účelem vymáhání práva nebo zpravodajské spolupráce bude mít pravděpodobně vliv na posuzovaný korejský právní rámec pro ochranu údajů.

22. EDPB konstatuje, že dohled nad vymáháním trestního práva a nad vnitrostátními bezpečnostními orgány je zajištěn kombinací různých interních a externích orgánů, zejména korejskou komisí pro ochranu osobních údajů (PIPC), která má dostatečné výkonné pravomoci.

23. Účinné prostředky nápravy vyžadují, aby se subjekty údajů mohly obrátit na příslušný orgán, který splňuje požadavky článku 47 Listiny základních práv Evropské unie (dále jen „**Listina**“), tj. orgán, který je příslušný určit, zda zpracování údajů probíhá, a ověřit zákonnost zpracování údajů a který má vymahatelné nápravné pravomoci v případě, že je zpracování údajů nezákonné. V této souvislosti EDPB žádá Evropskou komisi, aby objasnila, zda se na stížnost u korejské komise pro ochranu osobních údajů (PIPC) nebo na jakoukoli žalobu u soudu vztahují hmotněprávní a/nebo procesní požadavky, například důkazní břemeno, a zda by jednotlivci v EHP byli schopni daný předpoklad splnit.

1.3. Závěr

24. EDPB se domnívá, že toto rozhodnutí o odpovídající ochraně má zásadní význam i s přihlédnutím k tomu, že – až na výjimky uvedené v tomto stanovisku – bude zahrnovat předávání údajů ve veřejném i soukromém sektoru.

25. EDPB vítá snahy ze strany Evropské komise a korejských orgánů uvést korejský právní rámec do souladu s právním rámcem evropským. Zlepšení, která mají být zavedena oznámením č. 2021-1, k překlenutí některých rozdílů mezi těmito dvěma rámci, jsou velmi důležitá a dobře přijímaná. EDPB

však konstatuje, že řada obav, mimo jiné v souvislosti s oznámením č. 2021-1, spolu s potřebou dodatečného objasnění dalších otázek, přetrvává, a doporučuje Evropské komisi, aby se obavami a žádostmi o objasnění vznesenými EDPB zabývala a aby poskytla další informace a vysvětlení k otázkám nastoleným v tomto stanovisku.

2. ÚVOD

2.1. Korejský rámec pro ochranu údajů

26. Hlavním právním předpisem upravujícím ochranu údajů v Korejské republice je zákon o ochraně osobních údajů (zákon č. 10465 ze dne 29. března 2011, naposledy pozměněný zákonem č. 16930 ze dne 4. února 2020, dále jen „**zákon PIPA**“). Zákon je doplněn prováděcí vyhláškou (prezidentská vyhláška č. 23169 ze dne 29. září 2011, naposledy pozměněná prezidentskou vyhláškou č. 30892 ze dne 4. srpna 2020, „prováděcí vyhláška k zákonu PIPA“), která je právně závazná a vymahatelná.

27. Kromě zákona PIPA zahrnuje korejský rámec pro ochranu údajů regulační „oznámení“ vydaná korejským dozorovým úřadem – komisí pro ochranu osobních údajů (dále jen „**komise PIPC**“), která stanoví další pravidla pro výklad a používání zákona PIPA. Nedávno komise PIPC přijala oznámení č. 2021-1 ze dne 21. ledna 2021 (kterým se změnilo předchozí oznámení č. 2020-10 ze dne 1. září 2020, dále jen „**oznámení č. 2021-1**“) o výkladu, používání a vymáhání některých ustanovení zákona PIPA. Toto oznámení konkrétně vyplynulo z diskusí o přiměřenosti vedených mezi korejskými orgány a Evropskou komisí. Oznámení obsahuje vysvětlení k používání konkrétních ustanovení zákona PIPA, včetně zpracování osobních údajů předávaných do Koreje na základě zamýšleného rozhodnutí o odpovídající ochraně,[8] a *má status správního pravidla s právně závaznou platností pro správce osobních údajů v tom smyslu, že jakékoli porušení tohoto oznámení může být považováno za porušení příslušných ustanovení zákona PIPA*[9]. V této souvislosti by EDPB chtěl poznamenat, že navzdory tomu, že je oznámení v návrhu rozhodnutí označováno jako „doplňková pravidla“, neobsahuje další pravidla jako taková, ale spíše vysvětlení zaměřená na vyjasnění toho, jak by mělo být chápáno použití právního textu zákona PIPA, zejména s ohledem na údaje předávané z EHP. Za těchto okolností EDPB doporučuje pozorné sledování dodržování oznámení č. 2021-1 v praxi, zejména s ohledem na jeho uplatňování nejen ze strany komise PIPC, ale i soudy, zejména pokud je rovnocenná úroveň ochrany poskytovaná korejským právním rámcem založena na vysvětleních uvedených v oznámení č. 2021-1.

28. Další podstatné právní předpisy o ochraně údajů v korejském legislativním rámci stanoví pravidla pro zpracování osobních údajů v konkrétních průmyslových odvětvích, jako jsou:

- zákon o používání a ochraně úvěrových informací (dále jen „**zákon CIA**“), včetně jeho prováděcí vyhlášky (dále jen „**prováděcí vyhláška k zákonu CIA**“), která stanoví konkrétní pravidla použitelná pro komerční provozovatele a specializované subjekty (jako jsou ratingové agentury či finanční instituce) při zpracování osobních úvěrových informací nezbytných ke stanovení bonity účastníků finančních nebo obchodních transakcí,
- zákon o podpoře využívání informačních a komunikačních sítí a ochraně údajů (dále jen „**zákon o síti**“) a
- zákon o ochraně soukromí v komunikaci (dále jen „**zákon CPPA**“).

29. V oblasti přístupu vlády, kromě příslušných ustanovení obsažených v zákonech PIPA a CPPA, EDPB posoudil některé další právní předpisy, konkrétně zákon o trestním řízení („**CPA**“), zákon o podnikání

[8] Viz oddíl I přílohy I návrhu rozhodnutí.
[9] Tamtéž.

v telekomunikacích („**TBA**“), zákon o vykazování a používání specifikovaných informací o finančních transakcích (dále jen „**zákon ARUSFTI**“) a zákon o národní zpravodajské službě („**NISA**“).

2.2. Oblast působnosti posouzení provedeného EDPB

30. Návrh rozhodnutí Evropské komise je výsledkem posouzení korejského rámce pro ochranu údajů a následných diskusí s korejskou vládou. Podle čl. 70 odst. 1 GDPR se od EDPB očekává, že poskytne nezávislé stanovisko ke zjištěním Evropské komise, identifikuje případné nedostatky v právním rámci pro odpovídající ochranu a navrhne, jak je řešit.

31. Aby se předešlo opakování a za účelem poskytnutí pomoci při posuzování korejského právního rámce se EDPB rozhodl, že se zaměří na některé konkrétní body uvedené v návrhu rozhodnutí a poskytne k nim svou analýzu a stanovisko, přičemž se zdrží reprodukce většiny faktických zjištění a hodnocení, u nichž nemá důvody k předpokladu, že by právní předpisy Korejské republiky nebyly v zásadě rovnocenné právní předpisům v EHP. V souladu s judikaturou Soudního dvora Evropské unie se navíc velmi důležitá část analýzy zabývá právním režimem přístupu národní bezpečnosti k osobním údajům předávaným do Korejské republiky a praxí jejího vnitrostátního bezpečnostního aparátu.

32. Při posuzování EDPB zohlednil použitelný evropský rámec pro ochranu údajů, včetně článků 7, 8 a 47 Listiny, které chrání právo na soukromý a rodinný život, právo na ochranu osobních údajů a právo na účinnou nápravu a spravedlivý proces, a dále článku 8 Evropské úmluvy o lidských právech, který chrání právo na soukromý a rodinný život. EDPB vzal navíc v úvahu požadavky obecného nařízení o ochraně osobních údajů i příslušnou judikaturu.

33. Cílem této práce je poskytnout Evropské komisi stanovisko k posouzení přiměřenosti úrovně ochrany v Korejské republice. Pojem „odpovídající úroveň ochrany“, který již existoval podle směrnice 95/46, byl ještě více upřesněn Soudním dvorem Evropské unie. Je třeba připomenout standard stanovený Soudním dvorem Evropské unie ve věci Schrems I, a zejména, že ačkoli „úroveň ochrany“ ve třetí zemi musí být „v zásadě rovnocenná“ úrovni ochrany zaručené v EU, „*prostředky, které tato třetí země využívá v tomto směru k zajištění takovéto úrovně ochrany, [se] mohou lišit od prostředků zavedených v rámci EU*“[10]. Proto cílem není bod po bodu reflektovat evropské právní předpisy, nýbrž zjistit základní a hlavní požadavky, které zkoumané právní předpisy stanovují. Odpovídající úrovně lze dosáhnout kombinací práv pro subjekty údajů a povinností pro ty, kdo osobní údaje zpracovávají nebo nad tímto zpracováním vykonávají kontrolu, a dohledem ze strany nezávislých orgánů. Pravidla pro ochranu údajů jsou však účinná pouze v případě, jsou-li právně vymahatelná a dodržovaná v praxi. Proto je nutné zvážit nejen obsah pravidel vztahujících se na osobní údaje předané do třetí země nebo mezinárodní organizaci, ale také systém zavedený s cílem zajistit účinnost těchto pravidel. Účinné mechanismy prosazování jsou pro účinnost pravidel ochrany údajů nesmírně důležité[11].

2.3. Obecné připomínky a obavy

2.3.1. Mezinárodní závazky přijaté Korejskou republikou

34. Podle čl. 45 odst. 2 písm. c) GDPR a referenčního rámce pro odpovídající ochranu[12] vezme Evropská komise při posuzování odpovídající úrovně ochrany ve třetí zemi v úvahu mimo jiné mezinárodní závazky, které třetí země přijala, nebo jiné závazky vyplývající z účasti třetí země v mnohostranných či regionálních systémech, zejména pokud jde o ochranu osobních údajů, jakož i plnění těchto závazků.

[10] C-362/14 ze dne 6. října 2015, *Maximilian Schrems v. komisař pro ochranu údajů*, ECLI:EU:C:2015:650, bod 73–74.
[11] WP254, s. 2.
[12] WP254, s. 2.

35. Korea sje smluvní stranou několika mezinárodních dohod, které zaručují právo na soukromí, např. Mezinárodní pakt o občanských a politických právech (článek 17), Úmluva o právech osob se zdravotním postižením (článek 22) a Úmluva o právech dítěte (článek 16). Korea jako člen Organizace pro hospodářskou spolupráci a rozvoj (OECD) navíc dodržuje rámec OECD pro ochranu soukromí, zejména obecné pokyny upravující ochranu soukromí a přeshraniční toky osobních údajů.

36. EDPB rovněž bere na vědomí účast Koreje jako pozorovatelského státu na práci Poradního výboru Úmluvy Rady Evropy 108(+), ačkoli se Korea dosud nerozhodla, zda přistoupí.

2.3.2. Oblast působnosti rozhodnutí o odpovídající ochraně

37. Podle 5. bodu odůvodnění návrhu rozhodnutí dospěla Evropská komise k závěru, že Korejská republika zajišťuje odpovídající úroveň ochrany osobních údajů předávaných od správce nebo zpracovatele v Unii správcům (např. fyzickým nebo právnickým osobám, organizacím, veřejným institucím), kteří spadají do oblasti působnosti zákona PIPA, s výjimkou zpracování osobních údajů pro misijní činnosti náboženských organizací a pro jmenování kandidátů politickými stranami[13] nebo zpracování osobních úvěrových informací podle zákona CIA ze strany správců, kteří podléhají dohledu Komise pro finanční služby.

38. EDPB poznamenává, že rozhodnutí o odpovídající ochraně se bude vztahovat na předávání údajů z právního rámce EHP jak veřejným, tak soukromým „správcům osobních údajů“ spadajícím do působnosti zákona PIPA. EDPB chápe, že na subjekty jednající jako zpracovatelé údajů ve smyslu GDPR se také vztahuje pojem „správce osobních údajů“, protože zákon PIPA se na ně uplatní stejně, a že pro ně platí konkrétní povinnosti, pokud správce osobních údajů (tzv. outsourcer) zapojuje třetí stranu do zpracování osobních údajů (tzv. outsourcee). Aby se však předešlo nedorozuměním, EDPB Evropskou komisi vyzývá, aby objasnila, že rozhodnutí o odpovídající ochraně se bude vztahovat také na předávání údajů „zpracovatelům“ v Koreji a že ani v těchto případech nebude narušena úroveň ochrany osobních údajů předaných z EHP.

39. Navíc s ohledem na to, že rozhodnutí o odpovídající ochraně se vztahuje také na předávání osobních údajů mezi veřejnými orgány, EDPB chápe, že se to bude vztahovat i na předávání mezi orgány pro dohled nad ochranou údajů, a v zájmu jasnosti vyzývá Evropskou komisi, aby se touto otázkou konkrétně zabývala.

40. A dále pokud jde o subjekty vyloučené z oblasti působnosti rozhodnutí o odpovídající ochraně, EDPB by rád zdůraznil, že rozhodnutí o odpovídající ochraně by mohla prospět jasnější identifikace „obchodních organizací“, které podléhají dohledu komise PIPC (čl. 45 odst. 3 zákona CIA), aby správci údajů a jejich zpracovatelé v EHP mohli snadno posoudit, zda strana, která údaje přijímá, rovněž spadá do oblasti působnosti rozhodnutí o odpovídající ochraně, než předá údaje subjektům, které spadají do oblasti působnosti zákona CIA, nebo aby alespoň byli upozorněni na potřebu tento aspekt posoudit.

41. Pokud jde o rozsah rozhodnutí o odpovídající ochraně, EDPB z dodatečných vysvětlení Evropské komise vyrozuměl, že Korejská finanční zpravodajská jednotka (dále jen „**jednotka KOFIU**“), která je zřízena při Komisi pro finanční služby a dohlíží na prevenci praní peněz a financování terorismu podle zákona ARUSFTI[14], je rovněž vyloučena z oblasti působnosti, protože má jurisdikci pouze nad finančními institucemi, na které se návrh rozhodnutí nevztahuje. Ustanovení čl. 1 odst. 2 písm. c) návrhu rozhodnutí však z jeho působnosti vylučuje pouze ty správce osobních údajů, kteří podléhají dohledu Komise pro finanční služby a zpracovávají osobní úvěrové informace podle zákona CIA. V této souvislosti EDPB žádá Evropskou komisi, aby objasnila, zda jednotka KOFIU a činnosti zpracování údajů prováděné samotnou jednotkou KOFIU spadají do působnosti návrhu rozhodnutí.

[13] Další souvislosti viz níže v oddíle 3.1.2 tohoto stanoviska.
[14] Viz příloha II oddíl 2.2.3.1.

3. OBECNÉ ASPEKTY OCHRANY ÚDAJŮ

3.1. Zásady týkající se obsahu

42. Kapitola 3 referenčního rámce pro odpovídající ochranu je věnována „zásadám týkajícím se obsahu“. Systém třetí země musí tyto zásady zahrnovat, aby bylo možné považovat úroveň poskytované ochrany za v zásadě rovnocennou úrovni zaručené právními předpisy EU.

43. Ačkoli právo na ochranu osobních údajů jako takové není v korejské ústavě výslovně zakotveno, je uznáváno jako základní právo, odvozené z ústavních práv na lidskou důstojnost a usilování o štěstí (článek 10), soukromý život (článek 17) a soukromí komunikace (článek 18). To bylo potvrzeno jak Nejvyšším soudem, tak Ústavním soudem, jak je uvedeno v návrhu rozhodnutí Evropské komise[15]. EDPB bere toto uznání na vědomí, protože z něj odvozuje, že ochrana údajů jako základní právo podle článku 37 korejské ústavy *„může být omezena pouze zákonem a v případě potřeby z důvodu národní bezpečnosti nebo zachování zákona a pořádku nebo pro veřejné blaho“* a že *„i když jsou taková omezení uložena, nemohou ovlivnit podstatu svobody nebo práva“*.

44. Podle Evropské komise[16] Ústavní soud rozhodl, že i na cizí státní příslušníci se vztahují základní práva. Podle oficiálních prohlášení korejské vlády[17], ačkoli se judikatura dosud konkrétně nezabývala právem na soukromí nekorejských státních příslušníků, je mezi znalci všeobecně uznáváno, že články 12–22 ústavy stanoví „práva lidských bytostí“. Kromě toho Korejská republika přijala řadu právních předpisů v oblasti ochrany údajů, které poskytují záruky všem jednotlivcům bez ohledu na jejich státní příslušnost, jako např. zákon PIPA. V tomto ohledu EDPB bere na vědomí, že čl. 6 odst. 2 ústavy stanoví, že postavení cizích státních příslušníků je zaručeno podle mezinárodního práva a smluv a judikatury uvedené v návrhu rozhodnutí, podle něhož „cizinec“ může být nositelem „základních práv“. S ohledem na význam uznání práva na ochranu údajů u „cizích státních příslušníků“, EDPB upozorňuje Evropskou komisi na potřebu nadále sledovat judikaturu týkající se ochrany údajů jako základního práva uznávaného nejen pro korejské občany, ale pro všechny subjekty údajů, aby bylo zajištěno, že při předávání osobních údajů do Koreje na základě rozhodnutí o odpovídající ochraně nebude narušena úroveň ochrany fyzických osob zaručená GDPR.

3.1.1. Pojmy

45. Na základě referenčního rámce pro odpovídající ochranu podle GDPR by měly v právním rámci třetí země existovat základní pojmy nebo zásady ochrany osobních údajů. Ačkoli nemusí zcela odpovídat terminologii obecného nařízení o ochraně osobních údajů, měly by odrážet pojmy zavedené v evropských právních předpisech o ochraně údajů a být s nimi v souladu. Obecné nařízení o ochraně osobních údajů například obsahuje tyto důležité pojmy: „osobní údaje“, „zpracování osobních údajů“, „správce údajů“, „zpracovatel údajů“, „příjemce“ a „citlivé osobní údaje“[18].

46. Zákon PIPA obsahuje řadu definic, jako například definice „osobních údajů“, „zpracování“ a „subjektu údajů“, které se velmi podobají odpovídajícím pojmům podle GDPR.

3.1.1.1. *Pojem pseudonymizované údaje*

47. Ustanovení čl. 2 odst. 1 v rámci jiných definic uvedených v zákonu PIPA zejména definuje osobní údaje jako kterékoli z následujících informací týkajících se žijící osoby: a) informace, které identifikují konkrétní osobu podle jejího úplného jména, registračního čísla rezidenta, fotografie atd., a

[15] Viz 8. bod odůvodnění návrhu rozhodnutí a příslušná judikatura uvedená v poznámce pod čarou č. 10 návrhu rozhodnutí, u nichž jsou k dispozici pouze shrnutí v angličtině.
[16] Viz 9. bod odůvodnění návrhu rozhodnutí
[17] Viz oddíl 1.1. přílohy II návrhu rozhodnutí.
[18] WP254, s. 4.

b) informace, které, i když samy o sobě konkrétní osobu neidentifikují, lze snadno kombinovat s jinými informacemi, což vede k identifikaci konkrétní osoby. V tomto případě lze možnost takové kombinace určit s přihlédnutím k času, nákladům a technologii nezbytným pro identifikaci jednotlivce, například jako pravděpodobnost, že lze další potřebné informace získat.

48. Kromě toho podle čl. 2 odst. 1 písm. c) zákona PIPA jsou „pseudonymizované informace“ také považovány za osobní údaje. Pseudonymizované informace jsou definovány jako informace uvedené pod písmeny a) nebo b) výše, které jsou pseudonymizovány v souladu s pododstavcem 1–2, a tím přestávají umožňovat identifikaci konkrétní osoby bez použití informací pro obnovení původního stavu nebo jejich kombinací. Informace, které jsou plně anonymizovány, jsou vyloučeny z rozsahu použití zákona PIPA. Podle čl. 58 odst. 2 zákona PIPA se tento zákon nevztahuje na informace, které v kombinaci s jinými informacemi již neidentifikují určitou osobu, přičemž se přiměřeně zvažuje čas, náklady, technologie atd.

49. Evropská komise v 17. bodě odůvodnění svého návrhu rozhodnutí uvádí, že to odpovídá věcnému rozsahu použití GDPR a jeho pojmům „osobní údaje“, „pseudonymizace“ a „anonymizované informace“.

50. Podle čl. 28 odst. 7 zákona PIPA se články 20, 21, 27, čl. 34 odst. 1, články 35 až 37, čl. 39 odst. 3, čl. 39 odst. 4 a čl. 39 odst. 6–8 nevztahují na pseudonymizované osobní údaje.

51. Ve návrhu svého rozhodnutí Evropská komise uvádí, že čl. 28 odst. 7 zákona PIPA se vztahuje na pseudonymizované osobní údaje pouze tehdy, jsou-li zpracovávány pro účely statistiky, vědeckého výzkumu nebo archivace ve veřejném zájmu[19]. To však nevyplývá přímo z litery zákona, ale z vysvětlení uvedených v oznámení č. 2021-1[20]. Přestože EDPB uznává, že na základě struktury a odůvodnění zákona PIPA lze argumentovat, že by měl být čl. 28 odst. 2 zákona PIPA chápán a logicky vykládán tak, že se vztahuje také na čl. 28 odst. 7 zákona PIPA, s ohledem na důležitost oznámení č. 2021-1 při posuzování přiměřenosti úrovně ochrany osobních údajů v Korejské republice Evropskou komisí a aby se předešlo jakýmkoli pochybnostem, vyzývá EDPB Evropskou komisi, aby poskytla další informace o závaznosti, vymahatelnosti a platnosti oznámení č. 2021-1 a aby sledovala jeho použití v tomto konkrétním kontextu.

52. V této souvislosti by EDPB chtěl připomenout, že v rámci GDPR je pseudonymizace chápána jako doporučené bezpečnostní opatření. Jinými slovy, podle GDPR zůstávají pseudonymizované údaje osobními údaji, na které se GDPR plně vztahuje. Na základě výše uvedeného má EDPB obavy, že by při předání osobních údajů do Koreje mohla být narušena úroveň ochrany pseudonymizovaných osobních údajů nastavená v GDPR. EDPB proto navrhuje Evropské komisi, aby dále posoudila dopad pseudonymizace podle korejského práva a především to, jak může ovlivnit základní práva a svobody subjektů údajů, jejichž osobní údaje jsou předávány do Korejské republiky na základě rozhodnutí o odpovídající ochraně. EDPB proto vyzývá Evropskou komisi, aby poskytla ujištění, že úroveň ochrany osobních údajů od subjektů údajů v EHP nebude po předání údajů do Korejské republiky snížena, a to ani v případě, že jsou předané osobní údaje pseudonymizovány.

3.1.1.2. *Pojem správce osobních údajů*

53. Ustanovení čl. 2 odst. 5 zákona PIPA obsahuje definici „správce osobních údajů“, což znamená veřejnou instituci, právnickou osobu, organizaci nebo jednotlivce atd., který/která zpracovává osobní údaje přímo nebo nepřímo za účelem vedení souborů osobních informací *„jako součást své činnosti*“. V dodatečných zárukách uvedených v oznámení č. 2021-1 je však pojem správce osobních údajů

[19] Viz mimo jiné 82. bod odůvodnění návrhu rozhodnutí.
[20] Viz oddíl 4 přílohy I návrhu rozhodnutí.

definován jako veřejná instituce, právnická osoba, organizace, jednotlivec atd., který/která zpracovává osobní údaje přímo nebo nepřímo za účelem vedení souborů osobních údajů *„pro obchodní účely*“. Místo toho poznámka pod čarou č. 272 v návrhu rozhodnutí uvádí o pojmu správce osobních údajů následující: *„Jak je definováno v článku 2 zákona PIPA, tj. veřejná instituce, právnická osoba, organizace, jednotlivec atd., který/která zpracovává osobní údaje přímo nebo nepřímo za účelem vedení souborů osobních informací ‚pro oficiální nebo obchodní účely‘.“*

54. EDPB uznává, že tyto nesrovnalosti mohou být způsobeny překlady původního textu, jež poskytly korejské orgány, a vyzývá Evropskou komisi, aby pravidelně ověřovala kvalitu a spolehlivost překladů. EDPB však zdůrazňuje skutečnost, že k tomu, aby bylo možné posoudit zásadní rovnocennost úrovně ochrany údajů korejského právního rámce, je zapotřebí jasné porozumění účelům zpracování spadajících do věcné působnosti zákona PIPA. Dále v této souvislosti EDPB poznamenává, že zákon PIPA nepoužívá stejnou terminologii jako GDPR, pokud jde o pojem „správce“ a „zpracovatel“, a vyzývá Evropskou komisi, aby objasnila správnou definici a rozsah pojmu „správce osobních údajů“ a aby konkrétně řešila, zda tento pojem zahrnuje také zpracovatele ve smyslu GDPR, protože to přímo ovlivňuje rozsah působnosti rozhodnutí o odpovídající ochraně[21].

3.1.2. Částečné výjimky stanovené v zákonu PIPA

55. Ustanovení čl. 58 odst. 1 zákona PIPA vylučuje použití určitých částí zákona PIPA (tj. článků 15 až 57), pokud jde o čtyři kategorie zpracování osobních údajů, jak je popsáno níže. Tyto výjimky se týkají ustanovení zákona PIPA o konkrétních důvodech zpracování, určitých povinnostech v oblasti ochrany údajů, podrobných pravidel pro výkon individuálních práv a pravidel upravujících řešení sporů. EDPB však bere na vědomí, že některá obecná ustanovení zákona PIPA stále zůstávají použitelná, například ustanovení týkající se zásad ochrany údajů (článek 3 zákona PIPA) a individuálních práv (článek 4 zákona PIPA). Kromě toho čl. 58 odst. 4 zákona PIPA stanoví konkrétní povinnosti týkající se následujících čtyř kategorií zpracování údajů.

56. Zaprvé, částečná výjimka se týká osobních údajů shromážděných podle zákona o statistice ke zpracování veřejnými institucemi. Evropská komise v 27. bodě odůvodnění svého návrhu rozhodnutí uvádí, že podle objasnění obdržených od korejské vlády se osobní údaje zpracovávané v této souvislosti obvykle týkají korejských státních příslušníků a mohou jen výjimečně zahrnovat informace o cizincích, zejména v případě statistik o vstupu na území a odchodu z území, nebo o zahraničních investicích. Podle návrhu rozhodnutí však ani v těchto situacích nejsou tyto údaje obvykle předávány od správců/zpracovatelů v EHP, ale spíše je přímo shromažďují veřejné orgány v Koreji.

57. EDPB uznává odůvodnění Evropské komise ohledně výjimečnosti použití zákona o statistice na zpracování osobních údajů předávaných na základě rozhodnutí o odpovídající ochraně. Uvítal by však další informace a ujištění o konkrétních zárukách, které by byly použity v případě, že osobní údaje předané z EHP budou dále shromažďovány podle zákona o statistice ke zpracování veřejnými institucemi, zejména pokud jde o výkon individuálních práv subjekty údajů v souladu s čl. 89 odst. 2 GDPR, pokud je pravděpodobné, že taková práva nebudou znemožňovat nebo vážně narušovat dosažení konkrétních účelů a takové odchylky nejsou pro splnění těchto účelů nutné.

58. V tomto ohledu se zdá, že použití článku 4 zákona PIPA i na tento druh zpracování poskytuje jistoty, nicméně by EDPB uvítal v rozhodnutí o odpovídající ochraně dodatečné informace a objasnění konkrétních povinností podle čl. 58 odst. 4 zákona PIPA platných pro tyto činnosti zpracování, zejména pokud jde o minimalizaci údajů, omezené uchovávání údajů, bezpečnostní opatření a vyřizování stížností.

59. Zadruhé, částečná výjimka se týká osobních údajů shromážděných nebo požadovaných k poskytnutí pro analýzu informací souvisejících s národní bezpečností. EDPB si je vědom skutečnosti, že

[21] Viz rovněž odst. 38 výše.

v záležitostech národní bezpečnosti mají státy široký prostor k uvážení, který Evropský soud pro lidská práva uznává. EDPB rovněž poznamenává, že podle čl. 37 odst. 2 korejské ústavy nesmí jakékoli omezení svobod a práv, například ve věci nutné pro ochranu národní bezpečnosti, porušovat základní aspekt těchto svobod nebo práv. EDPB dále bere na vědomí záruky v oddíle 6 oznámení č. 2021-1 týkající se zpracování osobních údajů pro účely národní bezpečnosti, včetně vyšetřování porušení předpisů a vymáhání práva. V této souvislosti však EDPB vyzývá Evropskou komisi, aby dále vyjasnila rozsah výjimek, protože si klade otázku, zda jsou všechny výjimky stanovené v čl. 58 odst. 1 bodu 2 zákona PIPA (kapitoly III až VII) podstatné pro práci zpravodajských služeb a zda zajišťují rovnocennost se zásadami nezbytnosti a přiměřenosti. EDPB zejména vyzývá Evropskou komisi, aby poskytla podrobnější vysvětlení, za jakých okolností by se zpravodajská služba mohla na výjimky odkázat. EDPB považuje za nezbytné pečlivě sledovat dopad těchto omezení v praxi, zejména na účinné uplatňování a vymáhání práv subjektu údajů.

60. Zatřetí, částečná výjimka se vztahuje na „*osobní údaje zpracovávané dočasně, pokud jsou naléhavě nutné pro veřejnou bezpečnost, veřejné zdraví atd.*“ Podle 29. bodu odůvodnění návrhu rozhodnutí Evropské komise je tato kategorie vykládána komisí PIPC striktně a vztahuje se pouze na mimořádné události vyžadující naléhavá opatření, například ke sledování infekčních látek nebo k záchraně a pomoci obětem přírodních katastrof.

61. EDPB rovněž zdůrazňuje, že veškeré odchylky od úrovně ochrany osobních údajů by měly být vykládány striktně. EDPB zároveň konstatuje, že toto ustanovení není striktně definováno a neposkytuje vyčerpávající seznam příkladů situací, kdy by zpracování osobních údajů mohlo být považováno za „*naléhavě nutné*“. EDPB se například obává, zda by do této výjimky spadala také mezinárodní předávání zdravotních údajů během probíhající pandemie COVID-19. S ohledem na výše uvedené, EDPB vyzývá Evropskou komisi, aby poskytla další objasnění rozsahu této výjimky a aby pečlivě sledovala její uplatňování a rozsah, aby zajistila, že nepovede k tomu, že úroveň ochrany osobních údajů z EHP bude snížena po předání do Koreje na základě rozhodnutí o odpovídající ochraně.

62. Začtvrté, částečná výjimka se vztahuje na osobní údaje shromážděné nebo použité pro účely tiskových zpráv, misijní činnosti náboženských organizací a nominace kandidátů politickými stranami[22]. Pokud jde o zpracování osobních údajů tiskem pro novinářské činnosti, Evropská komise v 31. bodě odůvodnění svého návrhu rozhodnutí uvádí, že rovnováhu mezi svobodou projevu a jinými právy, včetně práva na soukromí, stanoví zákon o rozhodčím řízení a opravných prostředcích atd. za škody způsobené tiskovými zprávami (dále jen „**tiskový zákon**“) a komise uvádí konkrétní záruky, které z tiskového zákona vyplývají. EDPB však vyzývá Evropskou komisi, aby tuto výjimku a příslušnou judikaturu pečlivě sledovala, aby zajistila, že v praxi bude v korejském právním rámci zajištěna rovnocenná úroveň ochrany údajů.

3.1.3. Důvody pro zákonné a korektní zpracování pro legitimní účely

63. Podle referenčního rámce pro odpovídající ochranu musí být údaje v souladu s GDPR zpracovány zákonným, korektním a legitimním způsobem. Právní základ, podle něhož mohou být osobní údaje zákonně, korektně a legitimně zpracovány, by měl být stanoven dostatečně jasně. Evropský rámec uznává několik takových legitimních důvodů zpracování, jako jsou například ustanovení ve vnitrostátních předpisech, souhlas subjektu údajů, plnění smlouvy nebo legitimní zájem správce údajů nebo třetí strany, který nepřevažuje nad zájmy jednotlivce.

64. Zákon PIPA uvádí podle podobné struktury jako GDPR zásadu zákonnosti, korektnosti a transparentnosti úvodem (čl. 3 odst. 1 a 2 zákona PIPA), přičemž později stanoví zvláštní pravidla pro

[22] V souladu s tím je z působnosti rozhodnutí o odpovídající ochraně rovněž vyloučeno zpracování osobních údajů náboženskými organizacemi pro jejich misijní činnosti a zpracování osobních údajů politickými stranami v souvislosti s jmenováním kandidátů. Viz také odst. 37 v oddílu 2.3.2 výše.

její použití (články 15 až 19 zákona PIPA). Konkrétně článek 15 zákona PIPA obsahuje seznam právních důvodů, podle nichž mohou správci osobních údajů shromažďovat osobní údaje a používat je pro uvedené účely. Těmito právními důvody jsou 1) informovaný souhlas subjektu údajů; 2) zákonné povolení nebo nutnost splnění zákonné povinnosti; 3) nezbytnost pro výkon povinností veřejné instituce; 4) nezbytnost výkonu nebo plnění smlouvy se subjektem údajů; 5) nezbytnost ochrany životních, tělesných nebo majetkových zájmů subjektu údajů nebo třetí strany před bezprostředním nebezpečím (přičemž předchozí souhlas nelze získat); 6) nutnost dosáhnout oprávněného zájmu správce osobních údajů, který je nadřazený zájmu subjektu údajů.

65. Kromě toho článek 17 zákona PIPA uvádí právní důvody použitelné pro sdílení osobních údajů se třetí stranou, které zahrnují 1) informovaný souhlas subjektu údajů; 2) zákonné povolení nebo nutnost pro splnění zákonné povinnosti; 3) nezbytnost pro výkon povinností veřejné instituce; a 4) nezbytnost ochrany životních, tělesných nebo majetkových zájmů subjektu údajů nebo třetí strany před bezprostředním nebezpečím (přičemž předchozí souhlas nelze získat). I v případě absence souhlasu subjektu údajů je sdílení osobních údajů povoleno, pokud k tomu dochází v rozsahu přiměřeně souvisejícím s účely, pro které byly osobní údaje původně shromážděny (čl. 17 odst. 4 zákona PIPA).

66. Článek 18 zákona PIPA stanoví zvláštní pravidla pro používání a sdílení osobních údajů, pokud k tomu dojde mimo rozsah původního účelu shromažďování nebo poskytování. I v tomto případě je jedním z požadavků, mimo jiné, souhlas.

67. Přestože EDPB uznává značnou podobnost korejského práva s GDPR, pokud jde o zásadu zákonnosti a existenci obecného práva na pozastavení (článek 37 zákona PIPA), které lze rovněž uplatnit, pokud jsou osobní údaje zpracovávány na základě souhlasu, EDPB by rád upozornil na neexistenci obecného práva v rámci zákona PIPA na odvolání souhlasu[23]. S ohledem na důležitost souhlasu jako právního základu ve všech výše popsaných scénářích a s ohledem na úlohu individuálních práv v právním systému ochrany údajů pro účely ochrany základních práv a svobod subjektů údajů EDPB vyzývá Evropskou komisi, aby dále posoudila dopad neexistence obecného práva na odvolání souhlasu podle korejského práva a poskytla další záruky, které zajistí, že bude vždy zaručena základní úroveň ochrany údajů, jako je úroveň stanovená v GDPR, v případě potřeby také vyjasněním úlohy práva na pozastavení v tomto konkrétním kontextu.

3.1.4. Zásada účelového omezení

68. Referenční rámec pro odpovídající ochranu stanoví, v souladu s GDPR, že osobní údaje by měly být zpracovány pro konkrétní účel a následně použity pouze tehdy, pokud to není neslučitelné s účelem zpracování.

69. Podle čl. 3 odst. 1 a 2 zákona PIPA musí správci osobních údajů upřesnit a vyjasnit účely zpracování a zajistit, aby zpracování bylo s těmito účely slučitelné. Ačkoli je tato zásada potvrzena v jiných ustanoveních (totiž v čl. 15 odst. 1, čl. 18 odst. 1 a čl. 19 odst. 1 zákona PIPA), zpracování kvůli

[23] I když subjekty údajů mohou za určitých okolností souhlas odmítnout, viz například čl. 18 odst. 3 bod 5 zákona PIPA. Naproti tomu se zdá, že právo odvolat souhlas existuje pouze v konkrétních případech; podle čl. 27 odst. 1 bodu 2 zákona PIPA mají subjekty údajů právo odvolat souhlas, pokud si nepřejí, aby byly jejich osobní údaje předány třetí straně z důvodu převodu některých nebo všech činností správce osobních údajů, fúze atd.; podle čl. 39 odst. 7 mohou uživatelé PIPA kdykoli odvolat souhlas se shromažďováním, používáním a poskytováním osobních údajů od poskytovatele informačních a komunikačních služeb atd.; a podle článku 37 zákona CIA může jednotlivý subjekt úvěrových informací odvolat souhlas, který byl udělen poskytovateli či uživateli úvěrových informací.

„přiměřeně souvisejícím“ účelům je za určitých okolností povoleno (viz čl. 17 odst. 4 zákona PIPA)[24] stejně jako účelové používání a poskytování osobních informací (viz články 18 a 19 zákona PIPA)[25].

70. EDPB chápe, že v případě předávání osobních údajů z EHP do Korejské republiky na základě rozhodnutí o odpovídající ochraně představuje účel shromažďování správci se sídlem v EHP účel, pro který jsou údaje předávány, použitelný na zpracování korejským správcem osobních údajů, jenž údaje převzal. Změna účelu korejským správcem by byla povolena pouze podle čl. 18 odst. 2 bodů 1–3 zákona PIPA, *„pokud není pravděpodobné, že by to nekorektně zasáhlo do zájmu subjektu údajů nebo třetí strany“*[26]. V této souvislosti EDPB uznává prohlášení Evropské komise v 55. bodě odůvodnění návrhu rozhodnutí, že pokud právní předpisy povolují změny účelu, musí takové právní předpisy respektovat základní právo na soukromí a ochranu údajů. EDPB však konstatuje, že nebyly poskytnuty žádné konkrétní informace na podporu tohoto prohlášení, například nebyl učiněn žádný odkaz na článek 37 (korejské) ústavy. EDPB proto vyzývá Evropskou komisi, aby v návrhu rozhodnutí poskytla další ujištění a záruky, které zajistí, že všechny zákony, které povolují změnu účelu zpracování, budou vyžadovat dodržování základních práv a svobod subjektů údajů v oblasti soukromí a ochrany údajů.

3.1.5. Zásada kvality a přiměřenosti údajů

71. Referenční rámec pro odpovídající ochranu uvádí, že údaje by měly být přesné a v případě potřeby aktualizované. Údaje by měly být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovány.

72. Podle zákona PIPA musí správci zajistit, aby osobní údaje byly přesné, úplné a aktuální v rozsahu nezbytném ve vztahu k účelům, pro které jsou zpracovávány (čl. 3 odst. 3 zákona PIPA). Správci osobních údajů jsou povinni shromažďovat jen tolik osobních údajů, kolik je nutné k dosažení daného účelu. V tomto ohledu nesou důkazní břemeno (čl. 16 odst. 1 zákona PIPA).

73. V této souvislosti EDPB sdílí v tomto ohledu hodnocení Evropské komise, pokud jde o zásadní rovnocennost úrovně ochrany v rámci zákona PIPA ve srovnání s GDPR.

3.1.6. Zásada uchovávání údajů

74. Podle referenčního rámce pro odpovídající ochranu by údaje obecně neměly být uchovávány déle, než je nezbytné pro účely, pro které jsou osobní údaje zpracovávány. Jak je patrno z čl. 21 odst. 1 zákona PIPA, tato zásada existuje také v korejském právu. Podle zákona PIPA jsou správci osobních údajů povinni bez zbytečného odkladu zničit osobní údaje poté, co se po uplynutí doby uchovávání nebo po dosažení zamýšleného účelu zpracování stanou zbytečnými, pokud neplatí zákonné lhůty uchovávání.

75. EDPB je však znepokojen skutečností, že se čl. 21 odst. 1 zákona PIPA nevztahuje na pseudonymizované osobní údaje. EDPB si je vědom skutečnosti, že podle oddílu 4 bodu iii) oznámení č. 2021-1 platí, že „pokud správce osobních údajů zpracovává pseudonymizované údaje za účelem sestavování statistik, vědeckého výzkumu, uchovávání veřejných záznamů atd. a pokud nebyly pseudonymizované údaje zničeny poté, co byl splněn konkrétní účel zpracování v souladu s článkem 37 ústavy a článkem 3 (Zásady ochrany osobních údajů) zákona, správce tyto údaje anonymizuje s cílem zajistit, aby již neidentifikovaly konkrétního jednotlivce samy o sobě ani v kombinaci s jinými údaji, přiměřeně s ohledem na čas, náklady, technologii atd., v souladu s čl. 58 odst. 2 zákona PIPA.“ Vzhledem k tomu, že i zde je důležité oznámení 2021-1, a s ohledem na právní jistotu, pokud jde o rovnocennost úrovně ochrany osobních údajů předávaných do Korejské republiky podle rozhodnutí o

[24] Přitom je třeba předem ověřit slučitelnost účelu na základě kritérií stanovených v čl. 14 odst. 2 prováděcí vyhlášky k zákonu PIPA.
[25] Viz také odst. 66 výše.
[26] Čl. 18 odst. 2 zákona PIPA.

odpovídající ochraně, EDPB opakuje svou výzvu Evropské komisi, aby poskytla další informace konkrétně o tom, jak se oznámení č. 2021-1 stává závazným a jak je zajištěna jeho vymahatelnost a platnost[27].

3.1.7. Zásada zabezpečení a důvěrnosti údajů

76. Jak je popsáno v referenčním rámci pro odpovídající ochranu, zásada zabezpečení a důvěrnosti vyžaduje, aby subjekty zpracovávající údaje zajistily, že osobní údaje budou zpracovány způsobem, který zajistí jejich bezpečnost, včetně ochrany před neoprávněným nebo nezákonným zpracováním a před náhodnou ztrátou, zničením nebo poškozením, pomocí vhodných technických nebo organizačních opatření. Úroveň zabezpečení by se měla posuzovat podle aktuálního stavu vývoje a podle souvisejících nákladů.

77. Evropská komise identifikovala podobný princip zabezpečení údajů v čl. 3 odst. 4 zákona PIPA, který je dále upřesněn v článku 29 zákona PIPA. Kromě toho platí ustanovení o zabezpečení údajů, pokud správce osobních údajů zapojí třetí stranu (tzv. outsourcee). Bezpečnost zpracování musí být zajištěna technickými a manažerskými zárukami, které musí být rovněž obsaženy v závazné dohodě o zpracování údajů (článek 26 zákona PIPA a článek 28 prováděcí vyhlášky k zákonu PIPA). Dále podle zákona PIPA platí specifické povinnosti v případě porušení ochrany údajů, včetně povinnosti informovat dotčené subjekty údajů a dozorový úřad, pokud počet dotčených subjektů údajů překročí platnou prahovou hodnotu (článek 34 zákona PIPA ve spojení s článkem 39 prezidentské vyhlášky k zákonu PIPA), s výjimkou případů, kdy jsou dotčenými údaji pseudonymizované osobní údaje zpracovávané pro účely statistiky, vědeckého výzkumu nebo archivace ve veřejném zájmu (čl. 28 odst. 7 zákona PIPA). Také zde[28] má EDPB obavy z rozsáhlých výjimek pro pseudonymizované údaje a opakuje svou výzvu Evropské komisi, aby tento aspekt dále posoudila s cílem zajistit, že korejské právo stanoví v zásadě rovnocennou úroveň ochrany[29].

78. Bez ohledu na to je EDPB celkově spokojen s posouzením a závěrem Evropské komise, že je korejské právo s ohledem na zásadu bezpečnosti a důvěrnosti v zásadě rovnocenné.

3.1.8. Zásada transparentnosti

79. Na základě čl. 5 odst. 1 písm. a) GDPR je transparentnost základní zásadou systému ochrany údajů v EU. Ustanovení 39. bodu odůvodnění GDPR nastiňuje klíčovou funkci této zásady tím, že uvádí, že *„pro fyzické osoby by mělo být transparentní, že osobní údaje, které se jich týkají, jsou shromažďovány, používány, konzultovány nebo jinak zpracovávány, jakož i v jakém rozsahu tyto osobní údaje jsou či budou zpracovány. (...) Fyzické osoby by měly být upozorněny na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a jak mají v souvislosti s tímto zpracováním uplatňovat svá práva.“*

80. Referenční rámec pro odpovídající ochranu výslovně uvádí „transparentnost“ jako jednu ze zásad týkajících se obsahu, které je třeba zohlednit při hodnocení v zásadě rovnocenné úrovně ochrany poskytované třetí zemí. Přesněji uvádí, že *„každý jednotlivec by měl být informován o všech hlavních prvcích zpracování svých osobních údajů jasnou, snadno dostupnou, stručnou, transparentní a srozumitelnou formou. Tyto informace by měly zahrnovat účel zpracování, totožnost správce údajů, práva, která mu byla poskytnuta, a další informace, pokud je to nezbytné k zajištění spravedlnosti. Za určitých podmínek mohou existovat určité výjimky z tohoto práva na informace, například za účelem*

[27] Viz také odst. 51 výše v oddílu 3.1.1.1 tohoto stanoviska, jakož i odst. 52, které se týkají obecných obav EDPB ohledně vlivu pseudonymizace podle korejského práva.
[28] Jak již bylo popsáno v odst. 51–52 výše a v oddílu 3.1.1.1 tohoto stanoviska.
[29] Viz také oddíly 3.1.6 a 3.1.10 tohoto stanoviska.

ochrany vyšetřování trestných činů, národní bezpečnosti, soudní nezávislosti a soudních řízení nebo jiných důležitých cílů obecného veřejného zájmu, jako je tomu v případě článku 23 GDPR."

81. Podobně jako je tomu v případě GDPR, podle zákona PIPA existuje obecná zásada transparentnosti, která vyžaduje, aby správci osobních údajů zveřejnili své zásady ochrany osobních údajů a další záležitosti související se zpracováním osobních údajů (čl. 3 odst. 5 zákona PIPA). Zvláštní povinnosti informovat platí v případě, že se správci osobních údajů snaží získat od subjektů údajů souhlas se shromažďováním a zpracováním osobních údajů (čl. 15 odst. 2 zákona PIPA), se sdílením osobních údajů se třetí stranou (čl. 17 odst. 2 zákona PIPA) a pro účelové zpracování (čl. 18 odst. 3 zákona PIPA). Je pozoruhodné, že tyto informační povinnosti se také vztahují *mutatis mutandis* na zapojené třetí strany („outsourcee") (čl. 26 odst. 7 zákona PIPA).

82. EDPB uznává a vítá dodatečná ochranná opatření v oddílu 3 bodech i) a ii) oznámení č. 2021-1[30] týkající se informací, které mají být poskytnuty subjektům údajů při předání jejich údajů subjektem EHP, s přihlédnutím ke skutečnosti, že podle čl. 20 odst. 1 zákona PIPA, pokud údaje nebyly získány od subjektu údajů, jsou subjekty údajů informovány pouze na žádost, přičemž obecné právo být informován je uznáno pouze podle čl. 20 odst. 2 zákona PIPA, pokud některé operace zpracování překračují prahové hodnoty stanovené v prováděcí vyhlášce k zákonu PIPA (čl. 15 odst. 2).

83. Celkově je EDPB přesvědčen, že úroveň ochrany podle korejského práva, pokud jde o zásadu transparentnosti, je v zásadě rovnocenná s úrovní poskytovanou podle GDPR.

3.1.9. Zvláštní kategorie osobních údajů

84. Aby bylo uznáno, že systém ochrany údajů třetí země poskytuje úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni zajištěné GDPR, měly by existovat zvláštní záruky, pokud se jedná o zvláštní kategorie osob ve smyslu článků 9 a 10 GDPR.

85. Podle zákona PIPA se na zpracování takzvaných citlivých údajů vztahují zvláštní ustanovení, přičemž k těmto údajům patří osobní údaje odhalující ideologii, přesvědčení, vstup do odborové organizace nebo politické strany nebo vystoupení z nich, politické názory, zdraví, sexuální život a další osobní údaje, které pravděpodobně výrazně ohrozí soukromí subjektu údajů, a dále podle odkazu na prováděcí vyhlášku k zákonu PIPA též informace o DNA získané z genetického testování, údaje, které tvoří záznam v rejstříku trestů, osobní údaje vyplývající ze specifického technického zpracování údajů týkajících se fyzických, fyziologických nebo behaviorálních charakteristik jednotlivce za účelem jednoznačné identifikace této osoby a osobní údaje odhalující rasový nebo etnický původ.

86. Podobně jako GDPR i korejský zákon o ochraně údajů zakazuje zpracování citlivých údajů, pokud neplatí zvláštní výjimky, kterými je 1) informování subjektu údajů a získání konkrétního souhlasu a 2) právní ustanovení opravňující ke zpracování (čl. 23 odst. 2 zákonu PIPA) .

87. Na tomto základě EDPB v zásadě souhlasí se závěrem Evropské komise, že pokud jde o zpracování zvláštních kategorií osobních údajů, je korejské právo v zásadě rovnocenné. EDPB by však rád poznamenal, že ani v příručce k zákonu PIPA, ani ve vysvětleních od komise PIPC není stanoveno, zda je pojem „sexuální život" vykládán tak, že zahrnuje také sexuální orientaci jednotlivce nebo jeho preference, což nebylo zahrnuto v oznámení č. 2021-1. EDPB proto vyzývá Evropskou komisi, aby tyto informace poskytla za účelem jejich nezávislého posouzení. EDPB dále vyzývá Evropskou komisi, aby konkrétně citovala dokumenty, kde lze nalézt informace o tomto tématu, na které se odkazuje.

3.1.10. Právo na přístup, opravu, výmaz a námitku

88. V korejském právním rámci jsou práva subjektů údajů uznána v čl. 3 odst. 5 zákona PIPA, podle kterého správce osobních údajů musí zaručit práva subjektu údajů uvedená v článku 4 zákona PIPA a dále

[30] Příloha I návrhu rozhodnutí.

specifikovaná v článcích 35 až 37, 39 a čl. 39 odst. 2 zákona PIPA, a pokud jde o „osobní úvěrové informace“ (tj. úvěrové informace, které jsou nezbytné k určení bonity stran finančních nebo obchodních transakcí – viz 3. bod odůvodnění návrhu rozhodnutí), v článcích 37, 38 a čl. 38 odst. 3 zákona CIA.

89. EDPB poznamenává, že právo na přístup (a na opravu a výmaz, které může uplatnit „*subjekt údajů, který získal přístup ke svým osobním údajům podle článku 35 zákonu PIPA*“) může být omezeno nebo odepřeno v případech, „*kdy je přístup zakázán nebo omezen zákony*“, „*kdy může přístup způsobit poškození zdraví nebo těla třetí strany nebo neoprávněné porušení majetku a jiných zájmů jakékoli jiné osoby*“, a dále u veřejných institucí též v případech, kdy by poskytnutí přístupu „*způsobilo vážné potíže*“ při provádění určitých funkcí, dále specifikovaných v čl. 35 odst. 4 zákona PIPA[31]. Obdobná ustanovení obsahuje také článek 37 zákona PIPA týkající se práva na pozastavení zpracování osobních údajů.

90. Ustanovení článku 23 GDPR umožňuje prostřednictvím právních předpisů Unie nebo členského státu omezit jednotlivá práva, pokud takové omezení respektuje podstatu základních práv a svobod a je nezbytným a přiměřeným opatřením v demokratické společnosti a předpokládá, že tato omezení mimo jiné zajistí ochranu subjektů údajů nebo práva a svobody druhých a zajistí též „*monitorovací, inspekční nebo regulační funkci spojenou, i pouze příležitostně, s výkonem veřejné moci v případech uvedených v písmenech a) až e) a g) téhož článku*“.

91. Za těchto okolností by EDPB uvítal obecná ujištění v návrhu rozhodnutí o potřebě jakéhokoli zákona nebo statutu omezujícího práva subjektů údajů ke splnění požadavků korejské ústavy, že základní právo může být omezeno pouze tehdy, je-li to nezbytné pro národní bezpečnost nebo zachování práva a pořádku v oblasti veřejného blaha a že toto omezení nesmí ovlivnit podstatu dotčené svobody nebo práva (čl. 37 odst. 2 korejské ústavy).

92. Dále, pokud jde o výjimku týkající se „*neoprávněného zásahu do majetkových nebo jiných zájmů jakýchkoli jiných osob*“, EDPB uznává, že „*z toho vyplývá, že by mělo dojít k rovnováze mezi ústavně chráněnými právy a svobodami jednotlivce na jedné straně a druhých osob na straně druhé*“[32], nicméně vyzývá Evropskou komisi, aby pečlivě sledovala uplatňování této výjimky a příslušné judikatury s cílem zajistit, že v je rovnocenná úroveň ochrany práv subjektů údajů zajištěna korejským právním rámcem také v praxi.

93. Podobně by EDPB uvítal též pozorné sledování uplatňování výjimky pro veřejné orgány, zejména v případech, kdy by se uvažovalo, že by udělení přístupu způsobovalo „*vážné potíže*“ při plnění jejich povinností vzhledem k tomu, že tento výraz se zdá být širší než výraz používaný v jiných ustanoveních zákonu PIPA, např. v čl. 18 odst. 2 bodu 5[33], a měl by být vykládán restriktivně, aby se předešlo nepřiměřenému omezení práv subjektů údajů.

94. Kromě toho je EDPB znepokojen otázkou, zda jsou se zárukami stanovenými v evropském právním rámci v souladu výjimky, podle nichž se ustanovení týkající se transparentnosti na vyžádání (článek 20 zákona PIPA) a individuální práva (článek 35 až 37 zákona PIPA) – jakož i podobné výjimky týkající se požadavků na poskytovatele informačních a komunikačních služeb (čl. 39 odst. 2, čl. 39 odst. 6 až 8 zákona PIPA) a ty obsažené v zákonu CIA (viz výjimky stanovené v čl. 40 odst. 3 zákona CIA) – nevztahují na pseudonymizované informace, pokud jsou zpracovávány pro účely statistiky, vědeckého výzkumu nebo archivace ve veřejném zájmu (čl. 28 odst. 7 zákona PIPA).

[31] Stejné podmínky a výjimky z práva na přístup a opravu, které předpokládá zákon PIPA, platí také s ohledem na právo na přístup a opravu předpokládané zákonem CIA pro osobní úvěrové informace (poznámka pod čarou č. 135 návrhu rozhodnutí).

[32] 76. bod odůvodnění návrhu rozhodnutí.

[33] Pokud jde o výjimky z omezení neúčelného používání a poskytování osobních údajů, čl. 18 odst. 2 bod 5 zákona PIPA odkazuje na situace, kdy pro veřejné instituce „*není možné*“ vykonávat povinnosti.

95. Zdá se, že tato ustanovení zavádějí obecnou odchylku pro tento druh zpracování, zatímco GDPR předpokládá, že pokud jsou osobní údaje (včetně pseudonymizovaných osobních údajů) zpracovávány pro účely vědeckého nebo historického výzkumu nebo pro statistické účely, může právo Unie nebo členského státu stanovit odchylky od práva subjektu údajů, ale pouze „*pokud je pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění zvláštních účelů, a tyto odchylky jsou pro splnění těchto účelů nezbytné*“, přičemž pseudonymizace je pouze jedním z technických a organizačních opatření, která mají být přijata k zajištění dodržování zásady minimalizace údajů (čl. 89 odst. 1 GDPR).

96. Evropská komise považuje výjimku předpokládanou v čl. 28 odst. 7 zákona PIPA za oprávněnou i ve světle čl. 28 odst. 5 zákona PIPA, podle kterého je správci osobních údajů výslovně zakázáno zpracovávat pseudonymizované informace za účelem identifikace určité fyzické osoby, a odkazuje na přístup čl. 11 odst. 2 GDPR (ve spojení s 57. bodem odůvodnění GDPR) pro zpracování, které nevyžaduje identifikaci[34].

97. Podle článku 11 GDPR není správce povinen „*uchovávat, získávat nebo zpracovávat dodatečné informace za účelem identifikace subjektu údajů*“ pouze za účelem dodržování GDPR, pokud může pro zamýšlené účely zpracovávat osobní údaje, které nevyžadují nebo již nevyžadují identifikaci subjektu údajů; v takových případech, kdy je správce schopen prokázat, že není schopen identifikovat subjekt údajů, se práva subjektu údajů neuplatňují. Jak uznala Evropská komise[35], GDPR proto v takových případech vyžaduje „praktickou“ nemožnost u správce údajů a v souladu se zásadou minimalizace údajů uznává, že žádné další údaje nemusí být zpracovávány „kvůli“ GDPR.

98. EDPB však považuje tuto situaci za odlišnou od situace, kdy je správce prakticky schopen identifikovat subjekt údajů, ale není mu to umožněno zákonným ustanovením, jako je ustanovení obsažené v čl. 28 odst. 5 zákona PIPA. V tomto ohledu EDPB vítá vysvětlení poskytovaná komisí PIPC v oznámení č. 2021-1[36], které potvrzuje, že se oddíl 3 zákona PIPA (včetně čl. 28 odst. 7) a výjimka podle čl. 40 odst. 3 zákona CIA uplatňují pouze v případě, že jsou zpracovávány pseudonymizované informace pro vědecký výzkum, statistiku nebo archivaci ve veřejném zájmu. Kromě obav, které již byly zmíněny ohledně účinné závaznosti oznámení č. 2021-1[37], si EDPB však stále klade otázku, zda by odchylky stanovené v čl. 28 odst. 7 zákona PIPA a čl. 40 odst. 3 zákona CIA mohly být považovány za nezbytné a přiměřené v demokratické společnosti, pokud omezují práva subjektu údajů ve všech případech, kdy jsou pro takové účely zpracovávány pseudonymizované informace – tj. i když je správce osobních údajů prakticky schopen identifikovat subjekt údajů a práva pravděpodobně neznemožní nebo vážně nenaruší dosažení konkrétních účelů.

99. EDPB má zejména obavy, že tyto odchylky nebudou odůvodněné a bude nutné je dále zkoumat, obzvlášť pokud je použije správce osobních údajů, který pseudonymizuje údaje „*pro statistické účely, účely vědeckého výzkumu a archivace ve veřejném zájmu atd.*“ v souladu s čl. 28 odst. 2 zákona PIPA „*bez souhlasu subjektů údajů*“ (a bez poskytnutí informací, jak uvádí článek 20 zákona PIPA)[38], a pokud

[34] Je třeba poznamenat, že stejné odůvodnění by jako takové nebylo použitelné na výjimku stanovenou v čl. 40 odst. 3 zákona CIA pro zpracování pseudonymizovaných úvěrových informací, protože čl. 40 odst. 2 bod 6 předpokládá, že: *„Společnost poskytující úvěrové informace atd. nesmí zpracovávat pseudonymizované informace způsobem, kterým by bylo možné identifikovat konkrétního jednotlivce pro jakékoli ziskové nebo nekalé účely“*, což by mohlo umožnit opětovnou identifikaci pro spravedlivý účel, jako je např. žádost subjektu údajů.

[35] Viz 82. bod odůvodnění návrhu rozhodnutí.

[36] Viz oddíl 4 přílohy I návrhu rozhodnutí.

[37] Viz oddíl 3.1.1.1 výše.

[38] Viz čl. 28 odst. 7 zákona PIPA, jak je vysvětleno v oznámení č. 2021-1, podle kterého se určité záruky obsažené v zákonu PIPA, tj. „*články 20, 21, 27, čl. 34 odst. 1, články 35 až 37, čl. 39 odst. 3, čl. 39 odst. 4, čl. 39 odst. 6 až 8*“ nevztahují na pseudonymizované informace zpracovávané za účelem sestavování statistik, vědeckého výzkumu, uchovávání veřejných záznamů atd.

tento správce informace uchovává, což umožňuje opětovnou identifikaci. Podle GDPR by jednotlivci měli mít možnost uplatňovat svá práva s ohledem na jakékoli informace, které je dokážou identifikovat nebo rozeznat, i když jsou informace považovány za „pseudonymizované“, pokud neplatí již zmíněný článek 11 GDPR. V tomto ohledu EDPB poznamenává, že pouze v případě, kdy jsou tyto údaje poskytnuty třetí straně pro stejné statistické účely, účely vědeckého výzkumu a archivace, by neměly zahrnovat informace, které lze použít k identifikaci určité osoby, a tedy pouze správce osobních údajů, kterému jsou poskytovány pseudonymizované údaje podle čl. 28-2 odst. 2 zákona PIPA, by pravděpodobně „prakticky“ nebyl schopen identifikovat subjekt údajů bez dalších informací.

100. Stručně řečeno, vzhledem k tomu, že Evropská komise uznává, že „*místo aby se zákon PIPA spoléhal na pseudonymizaci jako možnou záruku, ukládá ji jako předpoklad pro provádění určitých činností zpracování pro účely statistiky, vědeckého výzkumu a archivace ve veřejném zájmu (například aby bylo možné zpracovávat údaje bez souhlasu nebo kombinovat různé soubory údajů)*“[39], ale v takových případech předpokládá důležitá omezení práv subjektů údajů, EDPB Evropskou komisi vyzývá, aby dále posoudila odchylky obsažené v čl. 28 zákona PIPA a čl. 40 odst. 3 zákona CIA a pozorně sledovala jejich uplatňování a příslušnou judikaturu[40], aby bylo zajištěno, že práva subjektů údajů nebudou nepřiměřeně omezována, pokud budou osobní údaje předávané podle rozhodnutí o odpovídající ochraně zpracovávány pro tyto účely, bereme-li přitom v úvahu, že tato práva v mnoha případech též pomáhají správci zajistit kvalitu zpracovávaných údajů.

3.1.11. Omezení dalšího předání

101. Referenční rámec pro odpovídající ochranu objasňuje, že úroveň ochrany fyzických osob, jejichž osobní údaje jsou předávány na základě rozhodnutí o odpovídající ochraně, nesmí být dalším předáním údajů narušena, a proto by jakékoli další předání „*mělo být povoleno pouze tehdy, pokud další příjemce (tj. příjemce dalšího předávání) podléhá rovněž pravidlům (včetně smluvních pravidel), která poskytují přiměřenou úroveň ochrany a dodržují příslušné pokyny při zpracování údajů jménem správce údajů*“.

102. Pokud jde o další předání třetím stranám (tj. „zpracovatelům“) usazeným v dalších třetích zemích, EDPB bere na vědomí, že v korejském právním rámci nejsou zavedena žádná zvláštní pravidla, která by se na tyto případy vztahovala, a že podle názoru Evropské komise[41] korejský správce osobních údajů musí zajistit soulad s ustanoveními zákona PIPA o outsourcingu (článek 26 zákona PIPA) prostřednictvím právně závazného nástroje a bude odpovědný za osobní informace, které byly předány třetím stranám (outsourcovány) (článek 26 zákona PIPA).

103. Pokud jde o další předávání třetím stranám (tj. jiným správcům osobních údajů), podle čl. 17 odst. 3 zákona PIPA musí korejský správce osobních údajů informovat subjekty údajů o předáních do zahraničí a získat jejich souhlas s těmito předáváními do zahraničí a „*nesmí uzavřít smlouvu o přeshraničním předávání osobních údajů v rozporu se zákonem PIPA*“. EDPB poznamenává, že toto poslední ustanovení zajistí – podle názoru Evropské komise[42], – že žádná smlouva o přeshraničním předávání nebude obsahovat závazky, které by odporovaly požadavkům kladeným zákonem PIPA na správce osobních údajů, a proto by mohla být považována za záruku, nicméně neukládá žádnou povinnost zavést ochranná opatření, která zajistí, že stejnou úroveň ochrany, jakou poskytuje zákon PIPA, bude poskytovat i příjemce údajů. EDPB proto uznává, že jako základ pro předávání údajů od korejského

[39] 42. bod odůvodnění návrhu rozhodnutí.
[40] Viz například ústavní výzvy Open Net (informace na internetových stránkách https://opennet.or.kr/19909 jsou k dispozici pouze v korejštině).
[41] 87. bod odůvodnění návrhu rozhodnutí.
[42] 88. bod odůvodnění návrhu rozhodnutí.

správce osobních údajů příjemci se sídlem ve třetí zemi bude obecně použit informovaný souhlas subjektu údajů.

104. V tomto ohledu jsou vítána dodatečná vysvětlení poskytovaná komisí PIPC v oznámení č. 2021-1 týkající se povinnosti informovat jednotlivce o třetí zemi, které budou jejich údaje poskytovány[43], protože – jak zdůrazňuje Evropská komise[44] – to by subjektům údajů v EHP pomohlo přijmout plně informované rozhodnutí o tom, zda souhlasit s přeshraničním předáváním údajů, či nikoli.

105. Jak je však rovněž uvedeno ve stanovisku 28/2018 k návrhu prováděcího rozhodnutí Evropské komise o odpovídající ochraně osobních údajů v Japonsku, je třeba zdůraznit, že podle GDPR musí být subjekty údajů výslovně informovány o možných rizicích takových převodů vyplývajících z absence odpovídající ochrany ve třetí zemi a neexistence vhodných záruk před souhlasem. Takové oznámení by mělo obsahovat například informace, že ve třetí zemi nemusí být dozorový úřad a/nebo že v ní nemusí být zajištěny zásady zpracování údajů a/nebo práva subjektů údajů[45]. Pro Evropský sbor pro ochranu osobních údajů je poskytnutí těchto informací nutné k tomu, aby měl subjekt údajů možnost udělit informovaný souhlas s plnou znalostí těchto konkrétních skutečností o předání[46]. EDPB má proto obavy ohledně zjištění Evropské komise v návrhu rozhodnutí o odpovídající ochraně, pokud jde o tento konkrétní druh předávání údajů. Subjekty údajů obvykle nemají znalosti o rámci pro ochranu údajů ve třetích zemích. Nelze tedy učinit závěr, že by subjekt údajů mohl posoudit riziko předávání údajů pouze na základě znalosti konkrétní země určení. Před souhlasem subjektu údajů musí spíše existovat jasné informace o konkrétních rizicích takového předání osobních údajů do země mimo území Korejské republiky.

106. EDPB proto vyzývá Evropskou komisi, aby zajistila, že informace, které mají být poskytnuty subjektu údajů „*o okolnostech souvisejících s předáním údajů*“, budou zahrnovat informace o možných rizicích předání vyplývajících z neexistence přiměřené ochrany ve třetí zemi a příslušných záruk. To je pro EDPB důležité, aby mohl posoudit, zda jsou požadavky na souhlas v zásadě rovnocenné s GDPR.

107. Vzhledem k tomu, že souhlas musí být poskytnut svobodně a musí být informovaný, konkrétní a jednoznačný, EDPB by uvítal ujištění v rámci rozhodnutí o odpovídající ochraně, že osobní údaje nebudou předávány od korejských správců osobních údajů do třetí země v žádné situaci, v níž by podle GDPR nemohl být udělen platný souhlas, např. kvůli nerovnováze sil.

108. U případů, kdy může správce osobních údajů poskytnout osobní údaje třetí straně v zahraničí bez souhlasu subjektu údajů – tj. 1) pokud jsou osobní údaje poskytovány v rozsahu přiměřeně souvisejícím s původním účelem shromažďování podle čl. 17 odst. 4 zákona PIPA; a 2) pokud mohou být osobní údaje poskytnuty třetí straně ve výjimečných případech uvedených v čl. 18 odst. 2 zákona PIPA – EDPB bere na vědomí objasnění poskytnutá komisí PIPC v oddíle 2 oznámení č. 2021-1 (a vítá předpokládané povinnosti uložené korejskému správci a zahraničnímu příjemci osobních údajů zajistit prostřednictvím právně závazného nástroje (jako je smlouva) úroveň ochrany rovnocennou se zákonem PIPA, a to i pokud jde o práva subjektu údajů).

3.1.12. Přímý marketing

109. Podle čl. 21 odst. 2 a 3 GDPR a podle referenčního rámce pro odpovídající ochranu musí mít subjekt údajů vždy možnost vznést námitku proti zpracování údajů za účelem profilování a přímého marketingu.

[43] Tamtéž.
[44] Tamtéž.
[45] Pokyny EDPB 2/2018 k výjimkám podle článku 49 nařízení (EU) 2016/679, 25. května 2018, s. 8.
[46] Pokyny EDPB 2/2018 k výjimkám podle článku 49 nařízení (EU) 2016/679, 25. května 2018, s. 7.

110. Pokud jde o právo na pozastavení stanovené v článku 37 zákona PIPA, EDPB uznává názor Evropské komise, že toto právo platí také tam, kde jsou údaje používány pro účely přímého marketingu[47]. EDPB by však uvítal další informace a vysvětlení v návrhu rozhodnutí v souvislosti s tímto posouzením, a zejména ohledně praktického uplatňování práva na pozastavení v rámci přímého marketingu (např. odkazy na příslušnou judikaturu atd.) V tomto ohledu by EDPB rovněž zdůraznil, že právo požádat poskytovatele/uživatele úvěrových informací, aby přestal kontaktovat subjekt údajů za účelem představení výrobků nebo služeb nebo vybízení k jejich nákupu, je výslovně stanoveno zákonem CIA (čl. 37 odst. 2).

111. Kromě toho, jak uznává Evropská komise[48], v korejském právním rámci takové zpracování obecně vyžaduje konkrétní (dodatečný) souhlas subjektu údajů (viz čl. 15 odst. 1 bod 1 a čl. 17 odst. 2 bod 1 zákona PIPA).

112. Vzhledem k tomu, že nelze vyloučit, že osobní údaje předané z EHP mohou být pro takové účely zpracovány v Koreji, EDPB by rovněž uvítal vyjasnění v rozhodnutí o odpovídající ochraně ohledně existence práva subjektu údajů odvolat souhlas[49] a práva nechat vymazat a dále nezpracovávat jeho osobní údaje, pokud je zpracování založeno na souhlasu (například v případě zpracování pro marketingové účely) a pokud subjekt údajů svůj souhlas odvolal.

3.1.13. Automatizované rozhodování a profilování

113. Jak Evropská komise uznala ve svém návrhu rozhodnutí[50], zákon PIPA a jeho prováděcí vyhláška neobsahují obecná ustanovení, která by řešila problém rozhodnutí, která ovlivňují subjekt údajů a která jsou založena výhradně na automatizovaném zpracování osobních údajů. Přesto korejský právní systém předpokládá takové právo v zákonu CIA, který obsahuje pravidla pro automatizovaná rozhodnutí (čl. 36 odst. 2), i když se zdá, že jejich uplatňování je mimo rozsah dohledu komise PIPC (a jako takový mimo rozsah použití tohoto návrhu rozhodnutí – viz část 2.3.2 výše o rozsahu použití návrhu rozhodnutí).

114. Jak již zvážila pracovní skupina zřízená podle článku 29[51] ve svém stanovisku 1/2016 k štítu pro ochranu soukromí a též EDPB ve svém předchozím stanovisku k rozhodnutí o odpovídající ochraně ve vztahu k Japonsku[52], rostoucí význam automatizovaného rozhodování, profilování a umělé inteligence v tomto ohledu dávají podnět k zaujetí přístupu, který by zaručoval vyšší ochranu. Na rozdíl od argumentů Evropské komise,[53] podle nichž absence zvláštních pravidel pro automatizované rozhodování v zákonu PIPA pravděpodobně neovlivní úroveň ochrany osobních údajů, které byly shromážděny v EU (protože jakékoli rozhodnutí založené na automatizovaném zpracování by obvykle přijal správce v EU, který má přímý vztah s dotčeným subjektem údajů), EDPB se domnívá, že nelze vyloučit, že by správce osobních údajů sídlící v Koreji mohl v případě údajů předaných na základě rozhodnutí o odpovídající ochraně použít automatizované rozhodování (například v souvislosti se zaměstnáním za účelem posouzení výkonu v práci, spolehlivosti, chování atd.)

[47] 79. bod odůvodnění návrhu rozhodnutí.
[48] Tamtéž.
[49] Viz také odst. 67 výše: Ačkoli čl. 37 odst. 1 zákona CIA jasně stanoví možnost odvolat souhlas, toto právo je v zákonu PIPA uvedeno pouze dvakrát za konkrétních okolností v čl. 27 odst. 1 bodu 2 a čl. 39 odst. 7.
[50] Viz 81. bod odůvodnění návrhu rozhodnutí.
[51] Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jednalo se o nezávislou evropskou poradní instituci v oblasti ochrany osobních údajů a soukromí. Její úkoly popisoval článek 30 směrnice 95/46/ES a článek 15 směrnice 2002/58/ES. Z pracovní skupiny zřízené podle článku 29 se nyní stal EDPB.
[52] Stanovisko 28/2018 k návrhu prováděcího rozhodnutí Evropské komise o přiměřené ochraně osobních údajů v Japonsku, přijaté dne 5. prosince 2018.
[53] 81. bod odůvodnění návrhu rozhodnutí.

115. Rozvoj nových technologií umožňuje společnostem snadněji zavést automatizované rozhodovací systémy nebo zvažovat jejich zavedení, což může vést k oslabení pozice jednotlivců. Pokud rozhodnutí učiněná výhradně těmito automatizovanými systémy mají dopad na právní situaci jednotlivců nebo je významně ovlivňují (například zařazením na černou listinu, čímž zbaví jednotlivce jejich práv), je klíčové zajistit dostatečné záruky včetně práva být informován o konkrétních důvodech, které jsou podkladem rozhodnutí, a o související logice, a práva na opravu nepřesných nebo neúplných informací a napadení rozhodnutí, pokud bylo přijato na nesprávném faktickém základě[54].

116. V této souvislosti má EDPB obavy ohledně nedostatku právních ustanovení o automatizovaném rozhodování v zákoně PIPA, a proto vyzývá Evropskou komisi, aby se touto obavou zabývala a nadále sledovala vývoj korejského legislativního rámce v tomto ohledu.

3.1.14. Odpovědnost

117. Korejský právní rámec obsahuje několik pravidel, jejichž cílem je zajistit, aby správci osobních údajů zavedli vhodná technická a organizační opatření k účinnému plnění svých povinností v oblasti ochrany osobních údajů a byli schopni toto dodržování prokázat, mimo jiné příslušnému dozorovému úřadu. EDPB zejména vítá existenci pravidel předpokládajících přijetí interního plánu řízení (článek 29 zákona PIPA), povinnost provést takzvané posouzení dopadu na soukromí („**PIA**“) v případech, kdy zpracování představuje vyšší riziko případného porušení ochrany osobních údajů (čl. 33 odst. 1 zákona PIPA a článek 35 prováděcí vyhlášky k zákonu PIPA), dále pravidel pro školení a dohled nad zaměstnanci (článek 28 zákona PIPA) a také povinnost určit pověřence pro ochranu osobních údajů (článek 31 zákona PIPA ve spojení s článkem 32 prováděcí vyhlášky k zákonu PIPA).

118. EDPB sdílí názor Evropské komise týkající se v zásadě rovnocenné ochrany, kterou zajišťují – a to i v případech, kdy se zdá, že se pravidla relativně liší od pravidel, která zahrnuje GDPR, např. neexistuje žádné ustanovení, které by stanovovalo potřebu nezávislosti pověřence pro ochranu osobních údajů, je však jasně stanoveno, že je podřízen vedení správce (čl. 31 odst. 4 zákona PIPA) a že nesmí být v důsledku výkonu těchto funkcí neoprávněně znevýhodňován (čl. 31 odst. 5 zákona PIPA) – a navrhuje, aby Evropská komise při přezkumu rozhodnutí o odpovídající ochraně sledovala skutečné uplatňování těchto ustanovení za účelem posouzení jejich účinného provádění.

3.2. Procesní a donucovací mechanismy

119. Na základě kritérií stanovených v referenčním rámci pro odpovídající ochranu analyzoval EDPB tyto aspekty korejského rámce pro ochranu údajů zahrnuté v návrhu rozhodnutí o odpovídající ochraně: existenci a fungování nezávislého dozorového úřadu, existenci systému zajišťujícího dobrou úroveň dodržování pravidel a systému přístupu k vhodným mechanismům nápravy, tak aby byly fyzické osoby z EHP vybaveny prostředky pro uplatňování svých práv a mohly se domáhat nápravy, aniž by čelily zatěžujícím překážkám v oblasti správní a soudní ochrany.

120. V souladu s kapitolou VI GDPR a kapitolou 3 referenčního rámce pro odpovídající ochranu musí existovat jeden nebo více nezávislých dozorových úřadů, jejichž úkolem je monitorovat, zajišťovat a prosazovat dodržování ustanovení o ochraně údajů a soukromí ve třetí zemi, aby byla zajištěna úroveň ochrany odpovídající úrovni ochrany v EHP.

121. V této souvislosti musí dozorový úřad třetí země jednat při plnění svých povinností a výkonu svých pravomocí zcela nezávisle a nestranně a nesmí při tom vyžadovat ani přijímat pokyny. Kromě toho by měl mít dozorový úřad všechny nezbytné a dostupné pravomoci a úkoly, aby zajistil dodržování práv na ochranu údajů a podporoval informovanost. Je třeba vzít v úvahu také zaměstnance a rozpočet dozorového úřadu. Dozorový úřad musí být rovněž schopen zahájit řízení z vlastního podnětu.

[54] WP 254, s. 7.

3.2.1. Příslušný nezávislý dozorový úřad

122. V Korejské republice je nezávislým orgánem odpovědným za dohled a vymáhání zákona PIPA komise PIPC. Komise PIPC se skládá z předsedy, místopředsedy a sedmi komisařů. Předsedu a místopředsedu jmenuje prezident na doporučení předsedy vlády. Z komisařů jsou dva jmenováni na doporučení předsedy, dva na doporučení zástupců politické strany, do které patří prezident, a tři zbývající členové jsou jmenováni na doporučení zástupců dalších politických stran (čl. 7 odst. 2 bod 2 zákona PIPA). Komisi PIPC je nápomocen sekretariát (čl. 7 odst. 13 zákona PIPA) Může zřizovat podkomise (skládající se ze tří komisařů) pro řešení drobných porušení a opakujících se záležitostí (čl. 7 odst. 12 zákona PIPA).

123. V tomto smyslu EDPB uznává, že komise PIPC navzdory své nedávné reorganizaci, která hluboce změnila její postavení a pravomoci, vynaložila značné úsilí při budování potřebné infrastruktury, která by vyhovovala provádění zákona PIPA a jeho nejnovějších změn. Mezi těmito snahami lze odkázat na stanovení pravidel komise PIPC, vypracování pokynů, které by poskytly vodítka k výkladu zákona PIPA, zřízení informační linky, která by radila provozovatelům podniků a jednotlivcům ohledně ustanovení o ochraně údajů, a zřízení zprostředkovatelské služby pro vyřizování stížností. Mezi úkoly komise PIPC patří zejména poradenství v oblasti zákonů a předpisů souvisejících s ochranou údajů, vytváření zásad a pokynů pro ochranu údajů, vyšetřování porušování práv jednotlivců, vyřizování stížností a zprostředkování sporů, vymáhání dodržování zákona PIPA, zajišťování vzdělávání a propagace v oblasti ochrany údajů a výměny a spolupráce s orgány pro ochranu údajů třetích zemí[55].

124. Jmenování a složení komise PIPC jsou stanoveny v čl. 7 odst. 2 zákona PIPA. Přestože komise PIPC spadá do pravomoci předsedy vlády (a předsedu a místopředsedu jmenuje prezident na doporučení předsedy vlády), právní rámec nařizuje, aby komisaři vykonávali své povinnosti nezávisle, v souladu se zákonem a svým svědomím. EDPB uznává institucionální a procesní záruky obsažené v zákonu PIPA a zejména v čl. 7 odst. 4 až 7. EDPB by nicméně uvítal, kdyby Evropská komise monitorovala veškerý vývoj, který by mohl ovlivnit nezávislost členů jihokorejského dozorového úřadu.

125. Návrh rozhodnutí navíc zatím neobsahuje analýzu rozpočtu komise PIPC, včetně zdrojů financování a transparentnosti rozpočtu. EDPB se domnívá, že tento prvek, který je uveden jak v čl. 56 odst. 1 GDPR, tak v zásadách ochrany údajů a jejich vymáhání a v mechanismech ochrany údajů, které je třeba při hodnocení systému země nebo mezinárodní organizace zohlednit v referenčním rámci pro odpovídající ochranu, musí být důkladně vzat v potaz, jelikož se jedná o ukazatel ekonomických a lidských zdrojů, které má dozorový úřad k dispozici k plnění svých zákonných povinností a úkolů v oblasti ochrany údajů nezávisle, a proto by EDPB doporučil Evropské komisi, aby to v návrhu rozhodnutí podrobněji zohlednila.

3.2.2. Existence systému ochrany údajů zajišťujícího dobrou úroveň souladu

126. V oblasti prosazování uznává EDPB rozsah donucovacích pravomocí a sankcí komise PIPC, jak jsou stanoveny v zákonech PIPA a CIA, a bere na vědomí objasnění uvedená v oznámení č. 2021-1, podle kterého se podmínky uvedené v čl. 64 odst. 1 zákona PIPA a čl. 45 odst. 4 zákona CIA[56] použijí vždy, když dojde k porušení některých ze zásad, práv a povinností obsažených v právních předpisech na ochranu osobních údajů. EDPB by však doporučil Evropské komisi, aby pečlivě sledovala uplatňování pravomocí komise PIPC nařídit v praxi porušovateli, aby přijal ta opatření uvedená v čl. 64 odst. 1 nebo čl. 45 odst. 4 zákona CIA, která komise považuje za vhodná.

127. Kromě toho, pokud jde o nápravná opatření stanovená v čl. 64 odst. 1 zákona PIPA, v případě nedodržení nápravného opatření je komise PIPC oprávněna uložit pokutu v maximální výši 50 milionů

[55] Úkoly a pravomoci komise PIPC jsou stanoveny zejména v čl. 7 odst. 8, čl. 7 odst. 9 a v článcích 61 až 66 zákona PIPA.

[56] Tzn. *„je pravděpodobné, že porušením zákona dojde k zásahu do práv a svobody fyzických osob ve vztahu k osobním údajům, a nečinnost pravděpodobně způsobí těžko napravitelnou škodu“.*

korejských wonů (čl. 75 odst. 2 bod 13 zákona PIPA). To odpovídá částce 36 564 EUR. EDPB se domnívá a má obavy, že takto omezený rozsah peněžních sankcí by nemusel mít na porušovatele zvlášť silný odrazující účinek, jak je zamýšleno zákonem s cílem zajistit prosazování pravidel ochrany údajů, protože částka se nezdá být dostatečně vysoká k odrazení, zejména v případě velkých organizací nebo podniků s významnými finančními zdroji.

128. S ohledem na možnost, že komise PIPC může požadovat, aby vedoucí ústřední správní agentury vyšetřoval správce osobních údajů nebo se společně zapojil do vyšetřování porušení zákona PIPA, a dokonce uložil nápravná opatření vůči správcům osobních údajů v jejich jurisdikci (čl. 63 odst. 4–5 zákona PIPA), EDPB poznamenává, že i když některé informace byly poskytnuty ve 122. bodě odůvodnění návrhu rozhodnutí, celkově zůstávají povaha těchto dalších agentur a jejich právní vztahy s komisí PIPC poněkud nejasné. Kromě toho čl. 68 odst. 1 zákona PIPA odkazuje na mnoho subjektů, na které by bylo možné delegovat pravomoci komise PIPC. I když se zdá, že toto ustanovení bylo použito pouze ve vztahu ke Korejské agentuře pro internet a bezpečnost[57], EDPB by uvítal objasnění s ohledem na povahu možných interakcí mezi těmito subjekty a pozorné sledování uplatňování tohoto ustanovení v budoucnu, aby byla zajištěna nezávislost subjektů pověřených uplatňováním pravidel ochrany údajů.

129. Pokud jde o sankce, zdá se, že korejský systém kombinuje různé druhy sankcí, od nápravných opatření a správních pokut až po trestní sankce, které budou mít pravděpodobně silný odrazující účinek. Korejské orgány dále předložily několik příkladů pokut nedávno uložených komisí PIPC – např. pokuta ve výši 6,7 miliardy korejských wonů uložená v prosinci 2020 jedné společnosti za porušení různých ustanovení zákona PIPA nebo pokuta ve výši 103,3 milionu korejských wonů udělená dne 28. dubna 2021 společnosti AI Technology za porušení pravidel zákonnosti zpracování, zejména souhlasu a zpracování pseudonymizovaných informací.

130. Přestože výše uvedené částky mohou mít odrazující účinek, EDPB by uvítal doplňující informace o metodě, kterou komise PIPC používá k výpočtu výše správních pokut, například pokud jde o pokuty uložené za nedodržení vydaného nápravného opatření podle čl. 64 odst. 1 zákona PIPA (viz čl. 75 odst. 2 bod 13 zákona PIPA). To je zvláště důležité v souvislosti s trestními sankcemi a uplatňováním (korejského) trestního zákona.

3.2.3. Systém ochrany osobních údajů musí subjektům údajů při výkonu jejich práv poskytovat podporu a pomoc a náležité mechanismy nápravy

131. Pokud jde o nápravu, zdá se, že korejský systém nabízí různé cesty k zajištění přiměřené ochrany a zejména vymáhání práv jednotlivců s účinnou správní a soudní nápravou, včetně náhrady škod.

132. Korejský systém rovněž nabízí alternativní mechanismy, které mohou jednotlivci využít za účelem získání nápravy, kromě správních a soudních cest, jak je vysvětleno v 132. a 133. bodu odůvodnění návrhu rozhodnutí, které se týkají telefonického střediska pro otázky soukromí a výboru pro zprostředkování sporů. Protože se jedná o dodatečné způsoby nápravy, EDPB by uvítal podrobnější vysvětlení, jak tyto mechanismy doplňují možnosti nápravy u komise PIPC a u soudů pro subjekty údajů, jejichž osobní údaje jsou předávány do Koreje podle rozhodnutí o odpovídající ochraně.

[57] Viz 117. bod odůvodnění návrhu rozhodnutí a článek 62 prováděcí vyhlášky.

4. PŘÍSTUP K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM Z EVROPSKÉ UNIE A JEJICH POUŽÍVÁNÍ VEŘEJNÝMI ORGÁNY V JIŽNÍ KOREJI

133. Pokud jde o hodnocení úrovně ochrany údajů v oblasti vymáhání práva a národní bezpečnosti, Evropská komise poskytla ve svém návrhu rozhodnutí a zpřístupněných přílohách komplexní informace. EDPB se proto v tomto stanovisku zdrží reprodukování většiny věcných zjištění a posouzení.

134. Evropská komise dochází k závěru, že ve výše uvedených oblastech existuje úroveň ochrany údajů, která odpovídá požadavkům stanoveným judikaturou Soudního dvora EU, a lze ji tedy považovat v zásadě za rovnocennou úrovni Evropské unie.

135. Jako obecnou poznámku by EDPB rád zdůraznil, že i v případech, kdy se zdá nebo kdy Evropská komise tvrdí, že údaje předávané z EU do Jižní Koreje pravděpodobně nebudou dotčeny příslušným korejským právem, je stále potřeba posoudit přiměřenost korejské úrovně ochrany údajů s ohledem na takové případy. O jejich relevanci svědčí i to, že se jimi v návrhu rozhodnutí zabývala i samotná Evropská komise.

4.1. Obecný rámec pro ochranu údajů v kontextu vládního přístupu k údajům

136. Pokud jde o přístup k osobním údajům ze strany veřejných orgánů, je třeba prozkoumat různé korejské právní předpisy, aby bylo možné posoudit úroveň ochrany práva na soukromí a ochrany údajů. EDPB předně konstatuje, že zákon PIPA jakožto klíčový zákon o ochraně údajů deklaruje širokou použitelnost. I když je však zákon PIPA plně použitelný v oblasti vymáhání práva, jeho použití na zpracování údajů pro účely národní bezpečnosti je omezené. Podle čl. 58 odst. 1 bodu 2 zákona PIPA se kapitoly III až VII nevztahují na zpracování osobních údajů pro účely národní bezpečnosti. Kapitoly I, II, IX a X však zůstávají použitelné i pro oblast národní bezpečnosti. Základní zásady zákona PIPA, jakož i základní záruky práv subjektů údajů a ustanovení o dohledu, vymáhání a opravných prostředcích se tedy vztahují na přístup a používání osobních údajů vnitrostátními bezpečnostními orgány.

137. Také jihokorejská ústava zakotvuje základní zásady ochrany údajů, konkrétně zásady zákonnosti, nezbytnosti a přiměřenosti. Tyto zásady se vztahují také na přístup jihokorejských veřejných orgánů v oblasti vymáhání práva a národní bezpečnosti k osobním údajům[58].

138. V oblasti vymáhání práva mohou policie, státní zástupci, soudy a další veřejné orgány shromažďovat osobní údaje na základě zvláštních právních předpisů, tj. zákona o trestním řízení („**CPA**“), zákona o ochraně soukromí v komunikacích („**CPPA**“), zákona o podnikání v telekomunikacích („**TBA**“) a zákona o oznamování a využívání stanovených informací o finančních transakcích („**ARUSFTI**“), který se vztahuje na stíhání praní špinavých peněz a financování terorismu a jejich předcházení. Tyto konkrétní zákony stanoví další omezení, záruky a výjimky.

139. V oblasti národní bezpečnosti může na základě zákona o národní zpravodajské službě („**NISA**“) a dalších „zákonů národní bezpečnosti“[59] shromažďovat osobní údaje a zachycovat komunikaci Národní zpravodajská služba („**NIS**“). EDPB chápe, že při výkonu svých pravomocí musí Národní zpravodajská služba dodržovat výše uvedená zákonná ustanovení i zákon PIPA.

140. EDPB žádá Komisi, aby objasnila, zda v Koreji existují další orgány kromě Národní zpravodajské služby, které jsou odpovědné za oblast národní bezpečnosti, protože v příloze I oddíle 6 Evropská komise navozuje dojem, že Národní zpravodajská služba je jedním z příkladů národní bezpečnostní agentury.

[58] Viz 145. bod odůvodnění návrhu rozhodnutí.

[59] Mezi zákony národní bezpečnosti patří například zákon o ochraně soukromí v komunikacích, zákon o boji proti terorismu na ochranu občanů a veřejné bezpečnosti nebo zákon o podnikání v telekomunikacích.

4.2. Ochrana a záruky pro údaje potvrzení komunikace v kontextu přístupu vlády k údajům pro účely vymáhání práva

141. Na základě příslušného zákona, zákona o ochraně soukromí v komunikacích, mohou orgány činné v trestním řízení přijmout dva typy opatření pro přístup ke komunikačním informacím. Zákon o ochraně soukromí v komunikacích rozlišuje opatření omezující komunikaci, která se týkají jak shromažďování obsahu běžné pošty a přímého odposlechu obsahu telekomunikací[60], tak shromažďování tzv. údajů potvrzení komunikace. Tyto údaje zahrnují datum telekomunikace, čas jejich zahájení a ukončení, počet odchozích a příchozích hovorů a také účastnické číslo druhé strany, frekvenci používání, soubory záznamů o používání telekomunikačních služeb a informace o poloze[61].

142. EDPB konstatuje, že údaje potvrzení komunikace zřejmě nevyužívají stejných záruk jako údaje shromažďované prostřednictvím opatření omezujících komunikaci, tj. obsahové údaje. Sbor EDPB si všímá, že shromažďování obsahu těží z více záruk než shromažďování údajů potvrzení komunikace pro účely vymáhání práva: Zaprvé, na rozdíl od shromažďování obsahových údajů se shromažďování údajů potvrzení komunikace neomezuje na vyšetřování určitých závažných trestných činů, ale může být prováděno, když je to považováno za nutné k provedení „jakéhokoli vyšetřování nebo výkonu jakéhokoli trestu“ (čl. 13 odst. 1 zákona o ochraně soukromí v komunikacích). Zadruhé, shromažďování údajů potvrzení komunikace v zásadě není strukturováno jako opatření poslední možnosti a má být použito pouze tam, kde je obtížné jinak zabránit spáchání trestného činu, zatknout zločince nebo shromáždit důkazy[62]. Údaje potvrzení komunikace lze shromažďovat vždy, když to státní zástupce nebo justiční policista „považuje za nutné“ pro vyšetřování trestného činu nebo výkon trestu. V tomto ohledu však existuje výjimka pro údaje sledované v reálném čase a pro údaje potvrzení komunikace týkající se konkrétní základnové stanice podle čl. 13 odst. 2 zákona o ochraně soukromí v komunikacích (CPPA). Zatřetí, orgány činné v trestním řízení, které shromažďují obsah komunikace, toho musí okamžitě zanechat, jakmile další přístup k údajům již není považován za nezbytný[63]. Pokud jde o údaje potvrzení komunikace, není to výslovně stanoveno v zákonu CPPA ani v jeho prováděcí vyhlášce.

143. EDPB bere na vědomí, že shromažďování údajů potvrzení komunikace může probíhat pouze na základě soudního příkazu. Zákon CPPA navíc vyžaduje, aby byly v žádosti o soudní příkaz i v samotném soudním příkazu uvedeny podrobné informace[64]. Takové předchozí soudní povolení slouží k omezení volného uvážení donucovacích orgánů při uplatňování práva a k ověření, zda v každém případě existují dostatečné důvody pro shromažďování údajů potvrzení komunikace. Sbor EDPB rovněž uznává, že právní předpisy Korejské republiky zřejmě nestanoví obecné a nerozlišující uchovávání údajů potvrzení komunikace. Přístup vlády k takovým údajům se tedy vždy týká údajů, které jsou nadále uchovávány pro účely fakturace a poskytování samotných komunikačních služeb.

144. EDPB však zdůrazňuje, že Soudní dvůr EU zpochybnil skutečnost, že by byly provozní údaje méně citlivé než ostatní, a zejména než obsahové údaje[65]. Vzhledem k tomu, že údajům potvrzení komunikace je

[60] Viz čl. 3 odst. 2, čl. 2 odst. 6, čl. 2 odst. 7 zákona o ochraně soukromí v komunikacích.
[61] Viz čl. 2 odst. 11 zákona o ochraně soukromí v komunikacích.
[62] To platí v případě obsahových údajů podle čl. 3 odst. 2 a čl. 5 odst. 1 zákona CPPA.
[63] Článek 2 prováděcí vyhlášky k zákonu CPPA.
[64] Viz 156. bod odůvodnění návrhu rozhodnutí.
[65] Viz rozhodnutí Soudního dvora EU ze dne 6. října 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, bod 71: *„Takové předání provozních a lokalizačních údajů bezpečnostním a zpravodajským službám představuje zásah do práva zakotveného v článku 7 Listiny, který musí být považován za zvlášť závažný, zejména s ohledem na citlivost informací, které z těchto údajů mohou vyplynout, a především na možnost vytvořit z nich profil subjektů údajů, neboť taková informace je stejně citlivé povahy, jako je samotný obsah sdělení. Navíc může v subjektech údajů vyvolávat dojem, že jejich soukromí je pod neustálým dohledem (obdobně viz rozsudky ze dne 8. dubna 2014, Digital Rights Ireland a další, C‑293/12 a C‑594/12, EU:C:2014:238, body 27 a 37, jakož i ze dne 21. prosince 2016, Tele2, C‑203/15 a C‑698/15, EU:C:2016:970, body 99 a 100).“*

v několika ohledech poskytována nižší úroveň ochrany než obsahovým údajům, EDPB vyzývá Evropskou komisi, aby pečlivě sledovala, zda záruky stanovené podle korejského práva pro takovou kategorii osobních údajů zajišťují úroveň ochrany v zásadě rovnocennou s úrovní ochrany zaručenou v EU, zejména s ohledem na přiměřenost a předvídatelnost práva.

4.3. Přístup korejských veřejných orgánů ke komunikačním informacím pro účely národní bezpečnosti

145. Pokud jde o právní rámec pro přístup národních bezpečnostních orgánů ke komunikačním informacím předávaným z EHP do Koreje, EDPB identifikoval dva problematické body, z nichž oba se týkají režimu přístupu ke komunikaci mezi nekorejskými státními příslušníky a spadají pod konkrétní soubor případů použití (viz odstavec 29). V těchto případech se některé záruky, které jsou jinak poskytovány, nevztahují na údaje potvrzení komunikace ani obsahové údaje. Jinými slovy, v těchto konkrétních případech se na tyto údaje nevztahují stejné záruky jako na sdělované údaje, pokud je do komunikace zapojen alespoň jeden korejský státní příslušník.

4.3.1. Žádná povinnost upozorňovat jednotlivce na přístup vlády ke komunikaci mezi cizími státními příslušníky

146. Ve výše uvedeném scénáři, tj. když žádná ze stran komunikace není korejským státním příslušníkem, nejsou národní bezpečnostní orgány povinny informovat jednotlivce o shromažďování a zpracování jejich údajů. EDPB uznává, že se tento problém týká pouze některých případů. Zaprvé, jak již bylo uvedeno, kdykoli je do komunikace zapojen alespoň jeden korejský státní příslušník, požadavky na oznámení podle zákona o ochraně soukromí v komunikacích se vztahují na všechny strany komunikace bez ohledu na jejich státní příslušnost[66]. Zadruhé, shromažďování osobních údajů pocházejících výhradně z komunikace mezi cizími státními příslušníky podléhá specifickému souboru případů použití. Právo na přístup se v takových případech vztahuje zejména na sdělení a) zemí nepřátelských vůči Korejské republice, b) zahraničních agentur, skupin nebo státních příslušníků podezřelých z účasti na protikorejských aktivitách[67] nebo c) členů skupin působících v rámci korejského poloostrova, ale fakticky mimo suverenitu Korejské republiky, a jejich zastřešujících skupin sídlících v cizích zemích. Komunikační sdělení mezi jednotlivci z EU předávané z EHP do Koreje tak lze shromažďovat pro účely národní bezpečnosti, pouze pokud spadají do jedné ze tří výše uvedených kategorií[68]. EDPB vyrozuměl z dodatečných vysvětlení Evropské komise, že dalším omezujícím faktorem je skutečnost, že platný právní rámec nestanoví zachycování údajů předávaných mimo Koreu.

147. Kritická povaha absence oznamovací povinnosti by proto mohla být z hlediska jejích praktických dopadů považována za omezenou. EDPB však zdůrazňuje význam (následného) oznámení o přístupu vlády, zejména s ohledem na zajištění účinných opravných prostředků. Podle Soudního dvora EU je oznámení „*nezbytné, aby dotčené osoby mohly vykonávat svá práva podle článků 7 a 8 Listiny požadovat přístup ke svým osobním údajům, které jsou předmětem těchto opatření, a případně dosáhnout jejich opravy či výmazu, jakož i využít v souladu s čl. 47 prvním pododstavcem Listiny účinné prostředky nápravy před soudem*“[69]. Vládní přístup pro účely národní bezpečnosti často zahrnuje tajná sledovací opatření, což znamená, že objekty sledování, subjekty údajů, si nejsou vědomy zpracování svých údajů. Tedy „*dotčená osoba má v zásadě jen malý prostor k tomu, aby se obrátila na soud, pokud není informována o opatřeních přijatých bez jejího vědomí, a nemá tudíž možnost napadnout jejich*

[66] Viz 192. bod odůvodnění návrhu rozhodnutí.
[67] Viz příloha II, poznámka pod čarou č. 244, podle které se pojem protikorejských činností vztahuje na činnosti, které ohrožují existenci a bezpečnost národa, demokratický řád nebo přežití a svobodu lidu.
[68] Viz 187. bod odůvodnění návrhu rozhodnutí.
[69] Rozsudek Soudního dvora EU ze dne 6. října 2020, spojené věci C-511/18, C-512/18 a C-520/18, *La Quadrature du Net a další*, ECLI:EU:C:2020:791, bod 190.

legalitu zpětně nebo pokud jakákoli osoba, která má podezření, že její komunikace je nebo byla odposlouchávána, nemá možnost se obrátit na soudy – pravomoc soudů tudíž nezávisí na oznámení odposlouchávanému subjektu, že došlo k odposlechu jeho komunikace“[70]. V této souvislosti a v souladu s tím EDPB mnohokrát vyjádřil své znepokojení nad účinnými opravnými prostředky v případech sledování. EDPB zdůrazňuje, že utajení vládních opatření nesmí vést k tomu, že taková opatření budou fakticky nezpochybnitelná. V této souvislosti je třeba v rámci celkového posouzení se zvláštním ohledem na poskytované mechanismy dohledu a nápravy podle korejského práva (viz body 4.7 a 4.8) rozhodnout, zda nedostatek oznamovací povinnosti u komunikace mezi cizími státními příslušníky má nebo nemá dopad na úroveň ochrany údajů, jak je posouzena v návrhu rozhodnutí.

148. Kromě toho EDPB v této souvislosti poznamenává, že zákon odkazuje na poměrně široké pojmy, jako jsou protikorejské nebo protinárodní činnosti[71], a že je obtížné předvídat, jak jsou tyto pojmy vykládány podle korejského práva. EDPB vyzývá Evropskou komisi, aby sledovala, jak jsou tyto podmínky konkretizovány v korejském právu a zda jejich uplatňování v praxi splňuje požadavky přiměřenosti vyplývající z práva EU.

4.3.2. Žádné předchozí nezávislé oprávnění ke shromažďování informací o komunikaci mezi cizími státními příslušníky

149. V případech, kdy mají být osobní údaje EHP odvozené z komunikace mezi nekorejskými státními příslušníky (a spadající do jednoho z výše uvedených případů použití) zpracovány v Koreji pro účely národní bezpečnosti, nepodléhá shromažďování těchto údajů předchozímu schválení nezávislým orgánem (jako je tomu v případě komunikace, kde alespoň jedna z dotčených osob je korejský státní příslušník).[72]

150. Zejména ve světle nedávných rozhodnutí Evropského soudu pro lidská práva („**ESLP**“) v případech „Big Brother Watch a další v. Spojené království“ a „Centrum för Rättvisa v. Švédsko“ považuje EDPB za nutné prozkoumat, zda jde v korejském rámci pro ochranu údajů o kritický nedostatek. V tomto ohledu EDPB připomíná, že jak bylo zdůrazněno v aktualizovaných doporučeních sboru o evropských základních zárukách pro kontrolní opatření,[73] čl. 6 odst. 3 Smlouvy o Evropské unii stanoví, že základní práva zakotvená v Evropské úmluvě o lidských právech představují obecné zásady práva EU, zatímco, jak připomíná Soudní dvůr EU ve své judikatuře, tato úmluva nepředstavuje právní nástroj, který byl formálně začleněn do práva EU, dokud k němu Evropská unie nepřistoupila[74]. Úroveň ochrany základních práv vyžadovaná v článku 45 GDPR tak musí být určena na základě ustanovení tohoto nařízení vykládaných ve spojení se základními právy zaručenými Listinou. Nicméně podle čl. 52 odst. 3 Listiny mají mít práva v ní obsažená, která odpovídají právům zaručeným Evropskou úmluvou o lidských právech, stejný význam a rozsah jako práva stanovená touto úmluvou. V důsledku toho je třeba vzít v úvahu judikaturu Evropského soudu pro lidská práva týkající se práv, která jsou rovněž

[70] Rozsudek Evropského soudu pro lidská práva ze dne 25. května 2021, *Big Brother Watch a další v. Spojené království*, ECLI:CE:ECHR:2021:0525JUD005817013, bod 337 a rozsudek Evropského soudu pro lidská práva ze dne 4. prosince 2015, *Roman Zacharov v. Rusko*, ECLI:CE: ECHR: 2015: 1204JUD004714306, bod 234.

[71] Evropská komise vysvětlila, že podle vysvětlení korejské vlády se to týká „činností, které ohrožují existenci a bezpečnost národa, demokratický řád nebo přežití a svobodu lidu“, viz také poznámka pod čarou č. 319 návrhu rozhodnutí o odpovídající ochraně.

[72] Viz 190. bod odůvodnění návrhu rozhodnutí.

[73] Viz doporučení EDPB 02/2020 o evropských základních zárukách pro kontrolní opatření, body 10, 11.

[74] Viz rozsudek SDEU ze dne 16. července 2020, C-311/18, *komisař pro ochranu osobních údajův. Facebook Ireland Ltd. a Maximilian Schrems*, ECLI:EU:C:2020:559 („Schrems II“), bod 98.

předpokládána v Listině, jako minimální hranici ochrany pro výklad odpovídajících práv v Listině, tj. v rozsahu, v jakém Listina, jak ji vykládá Soudní dvůr EU, neposkytuje vyšší úroveň ochrany[75].

151. EDPB konstatuje, že zatímco předchozí (nezávislé) schválení opatření pro sledování je považováno za důležitou ochranu proti svévoli, takové schválení nelze odvodit z judikatury Soudního dvora Evropské unie jako absolutního požadavku na přiměřenost kontrolních opatření. Evropský soud pro lidská práva však nyní výslovně stanovil požadavek na nezávislé povolení *ex ante* pro hromadné odposlechy[76]. I když to návrh rozhodnutí výslovně neuvádí, EDPB chápe, že právní rámec Korejské republiky nestanoví hromadné odposlechy, ale pouze cílené odposlechy telekomunikací[77]. Evropská komise tento výklad potvrdila.

152. Jak již bylo řečeno, výše uvedená rozhodnutí Evropského soudu pro lidská práva v souladu s judikaturou Soudního dvora EU[78] a předchozí judikaturou Evropského soudu pro lidská práva[79] opět ukazují důležitost komplexního dohledu nezávislých dozorových úřadů. EDPB zdůrazňuje, že nezávislý dohled ve všech fázích procesu vládního přístupu pro účely vymáhání práva a národní bezpečnosti je důležitou zárukou proti svévolným kontrolním opatřením, a tedy pro posouzení přiměřené úrovně ochrany údajů. Záruka nezávislosti dozorových orgánů ve smyslu čl. 8 odst. 3 Listiny má zajistit efektivní a spolehlivou kontrolu dodržování pravidel na ochranu fyzických osob v souvislosti se zpracováním osobních údajů. To platí zejména za okolností, kdy je vzhledem k povaze tajného sledování jednotlivci zabráněno požádat o přezkum nebo se přímo účastnit jakéhokoli přezkumného řízení před výkonem kontrolního opatření nebo během něj.

153. Absence předchozího nezávislého schválení nemůže být sama o sobě považována za podstatný nedostatek korejského práva, pokud jde o posouzení, zda je ochrana údajů v zásadě rovnocenná. Posouzení odpovídající ochrany opět závisí na všech okolnostech případu, zejména na účinnosti následného dohledu a právní nápravy, jak je stanoveno v právním rámci Koreje (viz další oddíly 4.7 a 4.8).

4.4. Dobrovolná poskytnutí informací

154. Podle čl. 83 odst. 3 zákona o podnikání v telekomunikacích (TBA) mohou poskytovatelé telekomunikačních služeb na požádání dobrovolně předávat takzvané „údaje o účastnících“[80] vnitrostátním bezpečnostním a donucovacím orgánům. I když EDPB shledává, že případy týkající se osobních údajů, které byly předány z EHP do Koreje, jsou pravděpodobně vzácné, je stále třeba je analyzovat, aby bylo možné posoudit úroveň ochrany údajů, jak již bylo uvedeno výše.

---

[75] Viz rozsudek Soudního dvora EU ze dne 6. října 2020, spojené věci C-511/18, C-512/18 a C-520/18, *La Quadrature du Net a další*, bod 124.

[76] Viz rozsudek Evropského soudu pro lidská práva ze dne 25. května 2021, *Big Brother Watch a další v. Spojené království*, ECLI:CE:ECHR:2021:0525JUD005817013, bod 351: „Hromadný odposlech by měl podléhat nezávislému povolení hned od začátku“, „hromadný odposlech by měl povolit nezávislý orgán; tedy orgán, který je nezávislý na výkonné moci”.

[77] Pouze text přílohy II oddílu 3.2 obsahuje výslovné prohlášení pro účely národní bezpečnosti, kde je uvedeno, že omezení a záruky *„zajišťují, že shromažďování a zpracování informací je omezeno na to, co je nezbytně nutné k dosažení legitimního cíle. To vylučuje jakékoli hromadné a paušální shromažďování osobních údajů pro účely národní bezpečnosti*“.

[78] Viz například rozsudek Soudního dvora EU, spojené věci C-203/15 a C-698/15, *Tele2 Sverige AB a další*, ECLI:EU:C:2016:970.

[79] Viz například rozsudek Evropského soudu pro lidská práva ze dne 4. prosince 2015, *Roman Zacharov v. Rusko*, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Dotyčnými soubory údajů by byly: jméno, rezidentské registrační číslo, adresa a telefonní číslo uživatelů, data, kdy uživatelé zahajují nebo ukončují své předplatné, jakož i identifikační kódy uživatelů (používané k identifikaci oprávněného uživatele počítačových systémů nebo komunikačních sítí).

155. EDPB chápe, že v těchto případech platí záruky ochrany údajů zákona PIPA a veřejné orgány – stejně jako poskytovatelé telekomunikačních služeb – musí tyto požadavky dodržovat[81] a že veřejné orgány i tito poskytovatelé mohou nést odpovědnost za jakékoli porušení práv a svobod dotčených subjektů údajů[82]. Kromě toho EDPB chápe, že poskytovatelé telekomunikačních služeb nejsou povinni těmto žádostem vyhovět.

156. S ohledem na koncepci přístupu vnitrostátních orgánů k údajům o účastnících pro účely vymáhání práva a zejména pro účely národní bezpečnosti prostřednictvím „dobrovolného poskytnutí informací“ ze strany provozovatelů telekomunikačních služeb však existuje obava ze zvýšeného rizika pro práva a svobody subjektů údajů, zejména s ohledem na jejich právo na informace.

157. Podle čl. 58 odst. 1 bodu 2 zákona PIPA se ustanovení kapitol III až VII nevztahují na žádné osobní informace, které mají být poskytnuty v souvislosti s národní bezpečností. V tomto ohledu se například na takové žádosti nepoužijí ustanovení článku 18 (Omezení neúčelového použití a poskytování osobních údajů) a článku 20 (Oznámení o zdrojích atd. osobních údajů shromažďovaných od třetích stran) zákona PIPA. V případech, kdy žádost podá vnitrostátní bezpečnostní orgán, to na jedné straně vyvolává otázku, zda čl. 58 odst. 1 bod 2 rovněž vylučuje uplatnění zákona PIPA na poskytovatele telekomunikačních služeb. Na druhé straně vyvstává otázka, zda se vyloučení použití článku 20 zákona PIPA v takových případech vztahuje i na odpovídající ustanovení obsažená v oddílu 3 přílohy I (Oznámení pro údaje, kdy osobní údaje nebyly získány od subjektu údajů (článek 20 zákona)). Pokud by tomu tak bylo a pokud by se čl. 58 odst. 1 bod 2 také vztahoval na poskytovatele telekomunikačních služeb, podle dostupných informací by existovalo riziko, že by nebyla zákonná povinnost informovat subjekty údajů o dobrovolném poskytnutí informací.

158. EDPB je proto znepokojen tím, že by vyžádání informací mohlo být neúčinné, což by značně ztížilo subjektům údajů uplatnění jejich práv na ochranu údajů, zejména pokud jde o soudní nápravu. V tomto ohledu EDPB vyzývá Evropskou komisi, aby objasnila rozsah příslušných ustanovení.

1.5. Další využití informací

159. Zásada omezení účelu je základním právním požadavkem ochrany údajů. Vyžaduje, aby byly osobní údaje shromažďovány pouze pro konkrétní, explicitní a legitimní účely a aby nebyly dále zpracovávány způsobem neslučitelným s těmito účely. Veřejné orgány jsou dále podle práva EU oprávněny zpracovávat osobní údaje za účelem prevence, vyšetřování nebo stíhání trestných činů, i když byly tyto údaje původně získány za jiným účelem, pokud veřejné orgány mají právní základ pro zpracování těchto údajů podle příslušných právních předpisů a pokud další zpracování není neúměrné[83].

160. V souladu s tím EDPB poznamenává, že korejský rámec ochrany údajů poskytuje podobné záruky a omezení, jaké poskytuje právo EU, pokud jde o další použití shromážděných informací pro účely vymáhání práva a národní bezpečnosti, např. zásada omezení účelu podle čl. 3 odst. 1 a 2 zákona PIPA.

1.6. Další předávání údajů a sdílení zpravodajských informací

161. Článek 44 GDPR stanoví, že předávání a další předávání osobních údajů se smí uskutečnit pouze v případě, že není narušena úroveň ochrany zaručená GDPR. Úroveň ochrany, která se vztahuje na osobní údaje předávané z EHP do Koreje, tedy nesmí být narušena dalším předáváním příjemcům ve třetí zemi, tj. další předávání by mělo být povoleno pouze v případě, že je zajištěno, že úroveň ochrany i nadále v zásadě odpovídá úrovni poskytované podle práva EU. Při posuzování, zda třetí země zajišťuje

[81] Viz 164. a 194. bod odůvodnění návrhu rozhodnutí.
[82] Viz 166. bod odůvodnění návrhu rozhodnutí.
[83] Viz čl. 4 odst. 2. směrnice o prosazování práva (LED).

odpovídající úroveň ochrany údajů, je proto nutné vzít v úvahu právní rámec země, do níž jsou údaje dále předávány. To je nesporné a v souladu s názorem Evropské komise[84] i EDPB.

162. V této souvislosti bere EDPB na vědomí, že Evropský soud pro lidská práva ve svých nedávných rozhodnutích „Big Brother Watch a další v. Spojené království" a „Centrum för Rättvisa v. Švédsko" poskytl pokyny[85] týkající se opatření na ochranu údajů, která je třeba dodržovat ve smluvních státech při předávání osobních údajů jiným stranám pro účely vymáhání práva a národní bezpečnosti v případech hromadného shromažďování údajů: *„Zaprvé, okolnosti, za kterých může k takovému předání dojít, musí být jasně stanoveny ve vnitrostátním právu. Zadruhé, předávající stát musí zajistit, aby přijímající stát při nakládání s údaji zavedl záruky schopné zabránit zneužití a nepřiměřeným zásahům. Přijímající stát musí zejména zaručit bezpečné skladování materiálu a omezit jeho další zpřístupňování. […] Zatřetí, zvýšená ochranná opatření budou nezbytná, když bude jasné, že je předáván materiál vyžadující zvláštní důvěrnost – např. důvěrný novinářský materiál."*[86]

163. Při uplatňování těchto standardů Evropský soud pro lidská práva ve věci „Centrum för Rättvisa v. Švédsko" shledal, že absence jakéhokoli výslovného právního požadavku v režimu odposlechu k posouzení nezbytnosti a přiměřenosti sdílení zpravodajských informací kvůli jeho možnému dopadu na právo na soukromí představuje porušení článku 8 Evropské úmluvy o lidských právech. Evropský soud pro lidská práva kritizoval, že v důsledku úrovně obecnosti práva by mohl být odposlechový materiál obecně zasílán do zahraničí, kdykoli je to podle uvážení v národním zájmu, bez ohledu na to, zda zahraniční příjemce nabízí přijatelnou minimální úroveň záruk[87].

164. EDPB uznává, že právní rámec Jižní Koreje neumožňuje hromadné odposlechy, stále s ohledem na důsledky judikatury Evropského soudu pro lidská práva, jak je uvedeno výše, a domnívá se, že kromě požadavků vyplývajících z práva EU, jak je vykládá Soudní dvůr EU, by argumenty Evropského soudu pro lidská práva měly být zváženy pro posouzení, zda právní rámec pro další předávání do třetí země poskytuje přiměřené standardy ochrany údajů.

4.6.1. Použitelný právní rámec pro další předávání údajů donucovacími orgány

165. Pokud jde o další předávání údajů příslušnými orgány pro účely vymáhání práva, EDPB z vysvětlení Evropské komise vyrozuměl, že se použije oddíl 2 přílohy I návrhu rozhodnutí o omezení dalšího předávání, a to i tehdy, když se předání uskuteční na základě jiného právního aktu než zákona PIPA. Podle tohoto pravidla platí, že *„pokud jsou osobní údaje poskytnuty třetí straně v zahraničí, nemusí se na ně vztahovat úroveň ochrany zaručená korejským zákonem o ochraně osobních údajů kvůli rozdílům v systémech ochrany osobních údajů v různých zemích. V souladu s tím budou takové případy považovány za „případy, kdy může dojít ke znevýhodnění subjektu údajů," uvedené v čl. 17 odst. 4 zákona nebo „případy, kdy je nečestně porušen zájem subjektu údajů nebo třetí strany," uvedené v čl. 18 odst. 2 zákona a čl. 14 odst. 2 prováděcí vyhlášky téhož zákona. Ke splnění požadavků těchto ustanovení proto musí správce osobních údajů a třetí osoba výslovně zajistit úroveň ochrany, která*

[84] Viz 84. a násl. bod odůvodnění návrhu rozhodnutí.

[85] Následující prvky byly stanoveny u příležitosti věci *Big Brother Watch* a věci *Centrum för Rättvisa*, které se týkají režimů hromadného odposlechu. Požadavek na preventivní opatření, která je třeba přijmout při předávání materiálu jiným stranám, byl již součástí kritérií vypracovaných Evropským soudem pro lidská práva v souvislosti s cíleným odposlechem a nebyl dále Evropským soudem pro lidská práva specifikován (viz věc *Big Brother Watch a další v. Spojené království*, bod 335, 362).

[86] Rozsudek Evropského soudu pro lidská práva ze dne 25. května 2021, *Big Brother Watch a další v. Spojené království*, ECLI:CE:ECHR:2021:0525JUD005817013, bod 362.

[87] Viz rozsudek Evropského soudu pro lidská práva ze dne 25. května 2021, *Centrum för Rättvisa v. Švédsko*, ECLI:CE:ECHR:2021:0525JUD003525208, bod 326.

odpovídá zákonu, včetně záruky výkonu práv subjektu údajů v právně závazných dokumentech, jako jsou smlouvy, rovněž i po předání osobních údajů do cizí země"[88].

166. EDPB vítá toto ustanovení, které za předpokladu odpovídající úrovně ochrany údajů v Koreji pro tento účel zajišťuje kontinuitu úrovně ochrany, kterou pro další předávání v zásadě poskytují i právní předpisy EU. Komise potvrdila názor EDPB, tedy že tento oddíl přílohy I se vztahuje na všechna další předávání údajů příslušnými orgány pro účely vymáhání práva. EDPB však zdůrazňuje, že je třeba zajistit, aby toto nařízení v praxi poskytovalo trvalou úroveň ochrany, protože může existovat nejistota ohledně toho, jaké smluvní záruky a závazky nebo jiné podobné mechanismy lze použít k dosažení takové úrovně ochrany v případě zpracování pro účely vymáhání práva. V tomto ohledu je třeba dodatečně například uvést, že osobní údaje lze ve třetí zemi sdílet pouze s relevantními příslušnými orgány.

167. S výhradou výše požadovaného objasnění, zda se návrh rozhodnutí vztahuje na jednotku KOFIU, EDPB poznamenává, že oficiální zastoupení pro vládní přístup[89] vysvětluje, že podle čl. 8 odst. 1 zákona ARUSFTI může komisař jednotky KOFIU poskytovat zahraniční finanční zpravodajské službě konkrétní informace o finančních transakcích, pokud je to považováno za nezbytné k dosažení účelu zákona ARUSFTI[90]. Článek 8 zákona ARUSFTI sám o sobě nestanovuje povinnost určit, zda cizí země poskytuje odpovídající záruky ochrany údajů, ani povinnost to zajistit. Příloha II v tomto ohledu neodkazuje na nový oddíl přílohy I. EDPB proto vyzývá Evropskou komisi, aby objasnila vzájemný vztah příslušné části přílohy I o omezení dalších předávání údajů a právního základu pro další předávání podle zákona ARUSFTI.

4.6.2. Použitelný právní rámec pro další předávání údajů pro účely národní bezpečnosti

168. Návrh rozhodnutí neobsahuje žádné informace o právním rámci pro další předávání údajů v oblasti národní bezpečnosti. EDPB chápe, že na rozdíl od předávání údajů pro účely vymáhání práva se oddíl 2 přílohy I nevztahuje na další předávání pro účely národní bezpečnosti. Články 17 a 18 zákona PIPA, které jsou předmětem dotyčného oddílu přílohy I, jsou součástí kapitoly III zákona PIPA, která se nevztahuje na zpracování osobních údajů pro účely národní bezpečnosti (čl. 58 odst. 1 zákona PIPA).

169. EDPB však předpokládá, že Korea může potřebovat předávat a také předává osobní údaje zahraničním zpravodajským službám pro účely národní bezpečnosti, např. za účelem spolupráce v boji proti přeshraničním hrozbám národní bezpečnosti, za účelem varování cizí vlády před těmito hrozbami nebo za účelem požádání cizí vlády o pomoc při identifikaci takových hrozeb.

170. EDPB chápe, že podle názoru Evropské komise jsou další předávání dostatečně upravena v korejském právu zárukami vyplývajícími z překlenujícího ústavního rámce, zejména zásadami nezbytnosti a přiměřenosti, jakož i základními zásadami ochrany údajů upravenými v zákoně PIPA, jako je zákonnost a spravedlnost zpracování, omezení účelu, minimalizace údajů, bezpečnost a obecné povinnosti zabránit zneužití osobních údajů či nesprávnému zacházení s nimi.

171. EDPB uznává obecnou použitelnost těchto klíčových zásad (ochrany údajů), ale vyjadřuje obavy, že tato ochranná opatření mají velmi obecnou povahu a konkrétně neodkazují na specifické okolnosti a podmínky pro další předávání údajů předaných z EHP pro účely národní bezpečnosti a ani se jimi v právním základě nezabývají. I když jsou tyto obecné a zastřešující zásady široce použitelné, EDPB si klade otázku, zda by to mohlo být považováno za splnění kritérií jasných a přesných pravidel a za

[88] Návrh rozhodnutí, příloha I, s. 7.

[89] Viz návrh rozhodnutí, příloha II.

[90] Viz návrh rozhodnutí, příloha II oddíl 2.2.3.2. I když k takové výměně může dojít pouze za podmínky, že zahraniční služba nesmí použít informace pro žádný jiný účel, než je původní účel poskytnutí údajů, a zejména ne pro trestní vyšetřování nebo soudní řízení (čl. 8 odst. 2 zákona ARUSFTI), komisař jednotky KOFIU může po obdržení žádosti cizí země udělit souhlas s použitím těchto údajů pro vyšetřování trestných činů nebo pro soudní řízení pro trestné činy s předchozím souhlasem ministra spravedlnosti (čl. 8 odst. 3 zákona ARUSFTI).

dostatečné zakotvení účinných a vymahatelných záruk. Zejména tam, kde je vládní přístup k osobním údajům a jejich zpracování tajné, a závěry, které lze z údajů vyvodit obzvláště závažné, je nezbytné mít jasná a podrobná pravidla. Zákon by měl dostatečně jasně stanovit rozsah jakékoli diskreční pravomoci svěřené příslušným orgánům a způsob jejího výkonu, aby jednotlivcům poskytl přiměřenou ochranu. V rozsudku *Schrems II* Soudní dvůr EU připomíná, že právní základ, který umožňuje zásah do základních práv, musí, aby byly splněny požadavky zásad nezbytnosti a přiměřenosti, sám definovat rozsah omezení výkonu dotčeného práva a stanovit jasná a přesná pravidla upravující oblast působnosti a uplatňování dotyčného opatření a uložit minimální ochranné záruky[91]. EDPB proto vyjadřuje obavy nad tím, že nestačí, aby takové záruky byly obecně zakotveny ve vyšších zákonech, aniž by byl konkrétně zaveden např. pojem přiměřenosti v samotném příslušném právním základu.

172. Tyto obavy podporuje i výše uvedené rozhodnutí Evropského soudu pro lidská práva, ve kterém soud konstatoval, že obecné pravidlo bez jakéhokoli výslovného požadavku na posouzení nezbytnosti a přiměřenosti nebo zvážení obav o soukromí není slučitelné s právem na soukromí podle článku 8 Evropské úmluvy o lidských právech. V tomto ohledu EDPB poznamenává, že v právu daného případu (stejně jako v právu Koreje) existují zastřešující (ústavou zaručené) zásady nezbytnosti a přiměřenosti, např. podle Listiny a prostřednictvím přistoupení k Evropské úmluvě o lidských právech.

173. EDPB vyzývá Evropskou komisi, aby objasnila právní základ ohledně toho, jak, do jaké míry a za jakých konkrétních podmínek jsou agentury zpravodajských služeb povinny zvážit soukromí a záruky ochrany údajů předtím, než zpřístupní osobní údaje pro účely národní bezpečnosti zahraničním partnerům. V případě, že taková povinnost vyplývá přímo z ústavních zásad, měla by Evropská komise dále posoudit požadavky na přesnost a jasnost příslušného zákona a potvrdit, že obecné ústavní zásady a zásady ochrany údajů jsou náležitě uplatňovány a prováděny.

4.6.3. Mezinárodní dohody

174. EDPB podotýká, že Evropská komise v rámci posouzení odpovídající ochrany nezohlednila existenci mezinárodních dohod uzavřených mezi Koreou a třetími zeměmi nebo mezinárodními organizacemi, které mohou stanovit zvláštní ustanovení pro mezinárodní předávání osobních údajů donucovacími orgány a/nebo zpravodajskou službou do třetích zemí. EDPB se domnívá, že uzavření dvoustranných nebo mnohostranných dohod se třetími zeměmi pro účely vymáhání práva nebo zpravodajské spolupráce pravděpodobně ovlivní právní rámec pro ochranu údajů v Koreji oproti tomu, jak byl posouzen.

175. EDPB proto vyzývá Evropskou komisi, aby objasnila, zda takové dohody existují, za jakých podmínek mohou být uzavřeny, a aby posoudila, zda ustanovení mezinárodních dohod mohou ovlivnit úroveň ochrany, která se vztahuje na osobní údaje předávané z EHP do Koreje prostřednictvím legislativního rámce, a praktiky v souvislosti s poskytováním údajů třetím zemím pro účely vymáhání práva a národní bezpečnosti.

4.7. Dohled

176. EDPB konstatuje, že dohled nad vymáháním trestního práva a vnitrostátními bezpečnostními orgány je zajištěn kombinací různých interních a externích orgánů.

177. V této souvislosti je třeba poznamenat, že Soudní dvůr EU opakovaně zdůraznil potřebu nezávislého dohledu jako základního prvku ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů. Pojem nezávislosti zahrnuje institucionální autonomii, osvobození od pokynů a materiální nezávislost. Aby bylo zajištěno důsledné sledování a prosazování práva na ochranu údajů, musí mít dozorové úřady účinné pravomoci, včetně opravných a nápravných pravomocí.

[91] Viz věc *Schrems II*, bod 175 a 180.

178. EDPB souhlasí se závěrem Evropské komise, že v celkovém hodnocení lze Koreu považovat za zemi s nezávislým a účinným systémem dohledu, přestože několik orgánů systému dohledu samo o sobě nesplňuje výše uvedené požadavky. Většina z nich například nemá výkonné pravomoci a omezuje se na pouhá doporučení, např. Národní komise pro lidská práva nebo Rada pro audity a inspekce. Kromě toho, mnohé příslušné veřejné orgány nejsou výlučně institucemi pro ochranu údajů, ale jsou obvykle pověřeny jinými úkoly v oblasti ochrany základních práv.

179. Na základě vysvětlení Evropské komise však EDPB poznamenává, že dohled nad orgány činnými v trestním řízení komplexně a bez výjimky zaručuje komise PIPC. Proto má komise PIPC vyšetřovací, nápravné a donucovací pravomoci podle zákona PIPA a dalších zákonů o ochraně údajů (např. zákona CPPA), které se vztahují na celou oblast přístupu k osobním údajům ze strany donucovacích orgánů a vnitrostátních bezpečnostních orgánů.

180. V této souvislosti by EDPB rád znovu zdůraznil, že pro výkon svých úkolů a pravomocí musí být dozorové úřady vybaveny dostatečnými lidskými, technickými a finančními zdroji. V tomto ohledu bohužel chybí informace o určených orgánech dohledu, zejména o komisi PIPC. EDPB proto opakuje svou žádost Evropské komisi o poskytnutí dalších informací v této věci.

181. Celkově by EDPB rád poznamenal, že v návrhu rozhodnutí nejsou téměř žádná prohlášení, příklady nebo čísla týkající se činností dohledu a vymáhání práva na ochranu údajů ze strany dozorových orgánů v oblasti vymáhání práva a národní bezpečnosti. Ty by byly užitečné v kontextu hodnocení účinnosti orgánů dohledu.

1.8. Soudní opravný prostředek a náprava

182. EDPB připomíná, že pro odpovídající úroveň ochrany údajů je zásadní, aby byly subjektům údajů poskytnuty komplexní opravné prostředky a možnosti nápravy v případě neoprávněného přístupu k údajům nebo jejich zpracování. Tyto opravné prostředky musí být dostatečné k tomu, aby umožnily subjektu údajů získat přístup k údajům o něm uloženým a požádat o jejich opravu nebo vymazání.

183. Ve světle rozsudků Soudního dvora EU ve věcech *Schrems I* a *Schrems II* je zřejmé, že kromě práva obrátit se na příslušné orgány má také účinná soudní ochrana ve smyslu čl. 47 odst. 1 Listiny zásadní význam pro předpoklad přiměřenosti práva třetí země.

184. EDPB bere na vědomí, že Korea zavedla různé způsoby výkonu práv jednotlivců na přístup, uchovávání, vymazání a pozastavení podle zákona PIPA. Tato práva lze uplatnit vůči samotnému správci nebo prostřednictvím stížnosti podané u komise PIPC nebo jiných orgánů dohledu, např. u Národní komise pro lidská práva. EDPB dále uznává možnost napadnout rozhodnutí správců nebo orgánů veřejné moci v reakci na jejich žádost na základě zákona o správních sporech.

185. Kromě toho EDPB z vysvětlení poskytnutých Evropskou komisí chápe, že jednotlivci mohou napadnout kroky donucovacích orgánů a národních bezpečnostních orgánů u příslušných soudů podle zákona o správním řízení a zákona o ústavním soudu a mají možnost získat náhradu škody podle zákona o státním odškodnění[92].

186. V této souvislosti má však EDPB obavy ohledně účinné nápravy pro jednotlivce z EU ve věcech týkajících se národní bezpečnosti v případě, kdy není dotčen žádný korejský občan. Jak je uvedeno v odstavci 33 a násl., vnitrostátní bezpečnostní orgány nejsou povinny oznamovat subjektům údajů shromažďování a zpracování jejich osobních údajů. Protože je v těchto případech podstatně obtížnější získat účinnou právní ochranu, EDPB by rád poukázal na to, že pokud se jedná o údaje předávané z EHP, jsou zde vyžadovány určité právní záruky. Tyto záruky musí subjektům údajů umožnit, aby mohly účinně zakročit proti nezákonnému zpracování údajů právně bezpečným způsobem, aniž by jim v tom bránily příliš úzké procesní požadavky, např. uvalení důkazního břemene, které nemohou splnit

[92] Viz příloha II oddíl 3.2.4 ve spojení s oddílem 2.4.3.

bez znalosti zpracování. Subjekty údajů dále musí mít možnost obrátit se na příslušný orgán, který splňuje požadavky článku 47 společného referenčního rámce, tj. který je příslušný určit, že dochází ke zpracování údajů, ověřit zákonnost zpracování a má prosaditelné nápravné pravomoci v případě nezákonného zpracování údajů. V tomto kontextu by například pouhé právo na stížnost ke korejské Národní komisi pro lidská práva nestačilo. EDPB proto vyzývá Komisi, aby podrobněji vysvětlila, jak jsou tyto požadavky prováděny z procesního a věcného hlediska, např. zda je možné, aby se subjekty údajů obrátily na komisi PIPC i na soud, aniž by musely prokazovat dané zpracování údajů.

187. Kromě toho EDPB poznamenává, že návrh rozhodnutí předpokládá mechanismus postoupení stížnosti, tj. že jednotlivci z EU mohou podat stížnost komisi PIPC prostřednictvím svého vnitrostátního orgánu pro ochranu údajů nebo EDPB. Jakmile je vyšetřování ukončeno, komise PIPC o tom jednotlivce informuje stejnou komunikační cestou[93]. EDPB vítá snahu o usnadnění přístupu k opravným prostředkům vůči korejským národním bezpečnostním orgánům. EDPB se zároveň zasazuje o to, aby takový postup postoupení byl směřován spíše prostřednictvím evropských vnitrostátních orgánů pro ochranu údajů než prostřednictvím EDPB, protože jsou příslušné a mají blíže k vyřizování jednotlivých stížností.

188. EDPB dále upozorňuje na možný rozpor, pokud jde o dobrovolné poskytnutí informací. Na jedné straně návrh rozhodnutí uvádí, že jednotlivci mohou získat nápravu v případě, že jsou jejich údaje poskytnuty protiprávně na základě žádosti o dobrovolné zpřístupnění, a to i vůči donucovacímu orgánu, který žádost vydal[94]. Na straně druhé návrh rozhodnutí odkazuje na požadavek přímého dopadu na právo jednotlivce napadnout kroky orgánů veřejné moci, přičemž uvádí (pouze) závazné žádosti o zveřejnění jako příklad pro případ, kdy se má za to, že správní opatření přímo ovlivňují právo na soukromí[95]. EDPB z vysvětlení Evropské komise chápe, že ve skutečnosti neexistuje žádné omezení možností opravných prostředků proti žádostem o dobrovolné poskytnutí informací, a proto žádá Evropskou komisi, aby to v rozhodnutí dále objasnila, a to jak v oblasti vymáhání práva, tak v oblasti národní bezpečnosti (na rozdíl od oddílu o vymáhání práva neobsahuje oddíl o dobrovolném poskytnutí informací pro účely národní bezpečnosti žádné výslovné prohlášení o nápravě v této souvislosti).

[93] Viz 205. bod odůvodnění a příloha I, s. 19 návrhu rozhodnutí.
[94] Viz 166. bod odůvodnění návrhu rozhodnutí.
[95] Viz 181. bod odůvodnění (vymáhání práva) a 208. a 181. bod odůvodnění (národní bezpečnost) návrhu rozhodnutí.