Stanovisko 14/2021 k návrhu vykonávacieho rozhodnutia Európskej komisie podľa nariadenia (EÚ) 2016/679 o primeranej ochrane osobných údajov v Spojenom kráľovstve

prijaté 13. apríla 2021

OBSAH

Európsky výbor pre ochranu údajov

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

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

so zreteľom na články 12 a 22 rokovacieho poriadku,

PRIJAL TOTO STANOVISKO:

1. ZHRNUTIE

1. Európska komisia 19. februára 2021 schválila návrh vykonávacieho rozhodnutia (ďalej len „návrh rozhodnutia“) o primeranej ochrane osobných údajov Spojeným kráľovstvom podľa všeobecného nariadenia o ochrane údajov[2]. Európska komisia následne začala postup jeho formálneho prijatia.

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

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

4. EDPB použil ako hlavný referenčný materiál pre túto prácu svoje referenčné kritérium primeranosti podľa všeobecného nariadenia o ochrane údajov[4] prijaté vo februári 2018 a odporúčania EPDB 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania[5].

[1] Odkazy na „členské štáty“ uvedené v tomto stanovisku by sa mali chápať ako odkazy na „členské štáty EHP“.
[2] Pozri tlačovú správu Európskej komisie Ochrana údajov: Európska komisia rieši bezpečnosť tokov osobných údajov do Spojeného kráľovstva, 19. február 2021, https://ec.europa.eu/commission/presscorner/detail/sk/ip_21_661.
[3] Tamže.
[4] Pozri Pracovnú skupinu zriadenú podľa článku 29, Referenčné kritérium primeranosti, prijaté 28. novembra 2017, naposledy revidované a prijaté 6. februára 2018, WP254 rev.01 (schválené EDPB, pozri https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (ďalej len „kritérium primeranosti podľa všeobecného nariadenia o ochrane údajov“).
[5] Pozri odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania, prijaté 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_sk.

1.1. Oblasti konvergencie

5. Hlavným cieľom EDPB je predložiť Európskej komisii stanovisko týkajúce sa primeranosti úrovne ochrany poskytovanej jednotlivcom v Spojenom kráľovstve. Treba si uvedomiť, že EDPB neočakáva, že právny rámec Spojeného kráľovstva preberie európske právne predpisy o ochrane osobných údajov.

6. Pripomína však, že na to, aby bol považovaný za právny rámec, ktorý poskytuje primeranú úroveň ochrany, sa v článku 45 všeobecného nariadenia o ochrane údajov a judikatúre Súdneho dvora Európskej únie (ďalej len „Súdny dvor EÚ“) vyžaduje, aby právne predpisy tretej krajiny boli v súlade s podstatou základných zásad zakotvených vo všeobecnom nariadení o ochrane údajov. Rámec ochrany údajov Spojeného kráľovstva je vo veľkej miere založený na rámci ochrany údajov EÚ [najmä všeobecné nariadenie o ochrane údajov a smernica Európskeho parlamentu a Rady (EÚ) 2016/680, ďalej len „smernica o presadzovaní práva EÚ“], ktorý vyplýva zo skutočnosti, že Spojené kráľovstvo bolo do 31. januára 2020 členským štátom EÚ. V zákone Spojeného kráľovstva o ochrane údajov z roku 2018, ktorý nadobudol účinnosť 23. mája 2018 a ktorým sa zrušil zákon Spojeného kráľovstva o ochrane údajov z roku 1998, sa okrem transpozície smernice o presadzovaní práva EÚ ďalej uvádza uplatňovanie všeobecného nariadenia o ochrane údajov v právnych predpisoch Spojeného kráľovstva, ako aj udeľovanie právomocí a ukladanie povinností vnútroštátnemu dozornému orgánu pre ochranu údajov, Úradu komisára pre informácie Spojeného kráľovstva (ďalej len „ICO“) [UK Information Commissioner's Office]. EDPB preto uznáva, že Spojené kráľovstvo vo svojom rámci ochrany údajov zväčša odzrkadľuje všeobecné nariadenie o ochrane údajov.

7. **Pri analyzovaní právnych predpisov a postupov tretej krajiny, ktorá bola donedávna členským štátom EÚ, je zrejmé, že EDPB identifikoval mnoho aspektov ako v podstate rovnocenných.**

8. EDPB poznamenáva, že v oblasti ochrany údajov je medzi rámcom všeobecného nariadenia o ochrane údajov a právnym rámcom Spojeného kráľovstva výrazný súlad v niektorých hlavných ustanoveniach, ako sú napríklad pojmy (napr. „osobné údaje“; „spracúvanie osobných údajov“; „prevádzkovateľ“); dôvody zákonného a spravodlivého spracúvania na legitímne účely; obmedzenie účelu; kvalita a primeranosť údajov; uchovávanie, bezpečnosť a dôvernosť údajov; transparentnosť; osobitné kategórie údajov; priamy marketing; automatizované rozhodovanie a profilovanie.

1.2. Výzvy

9. Spojené kráľovstvo bolo donedávna členským štátom EÚ; EDPB preto pri analýze jeho právnych predpisov a praxe zistil, že mnohé aspekty sú v podstate rovnocenné. EDPB sa súčasne so zreteľom na svoju úlohu v procese prijímania záverov o primeranosti, ale aj na časové obmedzenia, rozhodol zamerať svoju pozornosť na tie aspekty, pri ktorých sa domnieva, že je potrebné sa na ne bližšie pozrieť a podrobnejšie ich preskúmať.

10. Výzvy však naďalej pretrvávajú a EDPB sa domnieva, že nasledujúce položky treba ešte posúdiť, aby sa zabezpečila v podstate rovnocenná úroveň ochrany. Európska komisia by mala tieto položky v Spojenom kráľovstve pozorne monitorovať.

1.2.1. Všeobecné ustanovenia

11. Prvá všeobecná výzva sa týka monitorovania vývoja právneho systému Spojeného kráľovstva v oblasti ochrany údajov ako celku. Vláda Spojeného kráľovstva skutočne naznačila svoj zámer vypracovať samostatné a nezávislé politiky v oblasti ochrany údajov s prípadnou vôľou odchýliť sa od právnych predpisov EÚ o ochrane údajov. Takéto politické vyhlásenia sa v právnom rámci Spojeného kráľovstva zatiaľ neprejavili. Táto možná budúca **odchýlka by však mohla vytvárať riziká pre udržanie úrovne**

ochrany, ktorá sa poskytuje osobným údajom prenášaným z EÚ. Európska komisia sa preto vyzýva, aby tento vývoj od nadobudnutia účinnosti svojho rozhodnutia o primeranosti pozorne monitorovala a aby v prípade potreby prijala potrebné opatrenia vrátane zmeny a/alebo pozastavenia rozhodnutia.

1.2.2. Všeobecné aspekty ochrany údajov

12. Po prvé, takzvaná „**imigračná výnimka**“ stanovená v **časti 1** ods. 4 **prílohy 2 k zákonu o ochrane údajov z roku 2018** je **formulovaná „všeobecne“**. Ide o to, že sa uplatňuje aj v prípade, že osobné údaje nezhromažďuje na účely kontroly prisťahovalectva prevádzkovateľ, ale ich sprístupňuje ďalšiemu prevádzkovateľovi, ktorý tieto osobné údaje spracúva na účely kontroly prisťahovalectva.

13. EDPB vyzýva Európsku komisiu, aby overila súčasný stav konania vo veci *Open Rights Group & Anor, R ((On the Application Of)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* a, keďže tento rozsudok nie je právoplatný (prekážka rozhodnutej veci), aby overila, či je potvrdený alebo preskúmaný napadnutým rozsudkom, pričom zohľadní každú aktualizáciu v tejto súvislosti a uvedie ju v rozhodnutí. **EDPB takisto vyzýva Európsku komisiu, aby v rozhodnutí o primeranosti poskytla ďalšie informácie o imigračnej výnimke[6], najmä pokiaľ ide o nevyhnutnosť a proporcionalitu takejto širokej výnimky v práve Spojeného kráľovstva, hlavne so zreteľom na široký rozsah osobnej pôsobnosti.** EDPB zároveň vyzýva Európsku komisiu, aby ďalej preskúmala, či v právnom rámci Spojeného kráľovstva existujú ďalšie záruky, alebo či by sa o nich mohlo uvažovať, napríklad prostredníctvom právne záväzných nástrojov, ktoré by dopĺňali imigračnú výnimku zvýšením jej predvídateľnosti a záruk pre dotknuté osoby, čím by sa takisto umožnilo lepšie a urýchlené posúdenie a monitorovanie požiadaviek na nevyhnutnosť a proporcionalitu.

14. Po druhé, aj keď EDPB uznáva, že Spojené kráľovstvo vo svojom rámci ochrany údajov väčšinou zohľadnilo kapitolu V všeobecného nariadenia o ochrane údajov, EDPB určil určité aspekty právneho rámca Spojeného kráľovstva, **pokiaľ ide o následné prenosy**, ktoré by mohli ohroziť úroveň ochrany údajov prenášaných z EHP.

15. V článku 44 všeobecného nariadenia o ochrane údajov[7] sa skutočne ustanovuje, že prenosy a následné prenosy osobných údajov sa uskutočňujú len vtedy, ak nebude ohrozená úroveň ochrany fyzických osôb zaručená všeobecným nariadením o ochrane údajov. **To znamená, že nielen právne predpisy Spojeného kráľovstva budú „v podstate rovnocenné“ s právnymi predpismi EÚ, pokiaľ ide o spracúvanie osobných údajov prenášaných do Spojeného kráľovstva na základe budúceho rozhodnutia o primeranosti, ale aj to, že pravidlami platnými v Spojenom kráľovstve týkajúcimi sa následného prenosu týchto údajov do tretích krajín sa zabezpečí, že sa bude naďalej poskytovať v podstate rovnocenná úroveň ochrany.**

16. Hoci EDPB berie na vedomie schopnosť Spojeného kráľovstva podľa jeho právneho rámca uznať, že určité územia zabezpečujú primeranú úroveň ochrany údajov vzhľadom na rámec ochrany údajov Spojeného

---

[6] Aj ako výsledok priebežného preskúmania použitia imigračnej výnimky uvedený na s. 5 dôvodovej správy vlády Spojeného kráľovstva týkajúcej sa diskusií o primeranosti, oddiel E3: Príloha 2 Obmedzenia, 13. marca 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] *„Akýkoľvek prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácii, sa uskutoční len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky stanovené v tejto kapitole, ako aj ostatné ustanovenia tohto nariadenia vrátane podmienok následných prenosov osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny, alebo inej medzinárodnej organizácii. Všetky ustanovenia v tejto kapitole sa uplatňujú s cieľom zabezpečiť, aby sa neohrozila úroveň ochrany fyzických osôb zaručená týmto nariadením.“*

kráľovstva, EDPB chce zdôrazniť, že tieto územia nemusia mať dodnes prínos z rozhodnutia o primeranosti, ktoré vydala Európska komisia, a zabezpečovať úroveň ochrany „v podstate rovnocennú" s úrovňou zaručenou v EHP. Mohlo by to viesť k možným rizikám pri ochrane poskytovanej osobným údajom prenášaným z EHP, najmä ak sa v budúcnosti bude rámec ochrany údajov Spojeného kráľovstva odchyľovať od *acquis* EÚ. Spojené kráľovstvo okrem toho už uznalo za primerané tretie krajiny, ktoré požívajú závery o primeranosti Európskej komisie podľa smernice 95/46/ES[8], zatiaľ čo Európska komisia tieto závery čoskoro preskúma. K čomu pri tomto preskúmaní dospela, ešte nie je známe.

17. **Európska komisia by pri vyššie uvedených situáciách mala plniť svoju monitorovaciu úlohu a v prípade, že sa v podstate rovnocenná úroveň ochrany osobných údajov prenášaných z EHP nezachová, by Európska komisia mala zvážiť zmenu rozhodnutia o primeranosti s cieľom zaviesť osobitné záruky pre údaje prenášané z EHP a/alebo pozastaviť rozhodnutie o primeranosti.**

18. **Pokiaľ ide o medzinárodné dohody uzavreté medzi Spojeným kráľovstvom a tretími krajinami,** Európska komisia sa vyzýva, aby preskúmala vzájomné pôsobenie medzi rámcom ochrany údajov Spojeného kráľovstva a jeho medzinárodnými záväzkami nad rámec dohody o prístupe k elektronickým údajom na účely boja proti závažnej trestnej činnosti uzavretej medzi Spojeným kráľovstvom a Spojenými štátmi americkými (ďalej len „USA")[9] (ďalej len „dohoda medzi Spojeným kráľovstvom a USA o zákone CLOUD"), a najmä zabezpečila kontinuitu úrovne ochrany pri prenose osobných údajov z EÚ do Spojeného kráľovstva na základe rozhodnutia Spojeného kráľovstva o primeranosti v Spojenom kráľovstve, a následnom prenose do iných tretích krajín; a aby nepretržite monitorovala vývoj a v prípade potreby prijala opatrenia, ak by uzatvorenie medzinárodných dohôd medzi Spojeným kráľovstvom a tretími krajinami ohrozovalo úroveň ochrany osobných údajov poskytovanú v EÚ.

19. Európska komisia sa ďalej vyzýva, aby monitorovala, či sa dohodou medzi Spojeným kráľovstvom a USA o zákone CLOUD zaisťujú príslušné ďalšie záruky, a to s prihliadnutím na úroveň citlivosti dotknutých kategórií údajov a výhradné požiadavky na prenos elektronických dôkazov skôr priamo poskytovateľmi služieb než medzi orgánmi, pričom má posúdiť, za akých okolností možno primeraným vykonávaním prispôsobenej zastrešujúcej dohody medzi EÚ a USA poskytnúť záruky[10].

20. EDPB ďalej poznamenáva, že k následným prenosom môže dôjsť aj zo Spojeného kráľovstva do inej tretej krajiny na základe **nástrojov prenosu podľa platných právnych predpisov Spojeného kráľovstva na ochranu údajov[11]**. EDPB v nadväznosti na vec *Schrems II*[12] vyzýva Európsku komisiu, aby v rozhodnutí o primeranosti poskytla uistenia, že sa účinne zavedú nevyhnutné záruky, v ktorých sa zohľadnia aj právne predpisy prijímajúcej tretej krajiny.

21. Pokiaľ ide o absenciu **ochrany, ktorú poskytuje článok 48 všeobecného nariadenia o ochrane údajov**, v právnych predpisoch Spojeného kráľovstva, EDPB vyzýva Európsku komisiu, aby poskytla ďalšie záruky a konkrétne odkazy na právne predpisy Spojeného kráľovstva, ktoré zabezpečia, aby

[8] Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 23.11.1995, s. 31).
[9] Pozri Dohoda medzi vládou Spojeného kráľovstva Veľkej Británie a Severného Írska a vládou Spojených štátov amerických o prístupe k elektronickým údajom na účely boja proti závažnej trestnej činnosti, Washington DC, USA, 3. októbra 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.
[10] Pozri Dohoda o ochrane osobných informácií v súvislosti s predchádzaním trestným činom, ich vyšetrovaním, odhaľovaním a stíhaním, december 2016 (ďalej len „zastrešujúca dohoda medzi EÚ a USA")., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8.
[11] Pozri články 46 a 47 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.
[12] Pozri vec *Schrems II*.

úroveň ochrany podľa právneho rámca Spojeného kráľovstva bola v zásade rovnocenná s úrovňou ochrany zaručenej v EHP.

22. Čo sa týka **procesných mechanizmov a mechanizmov presadzovania**, EDPB berie na vedomie existenciu a efektívne fungovanie nezávislého dozorného orgánu; existenciu systému zabezpečujúceho dobrú úroveň súladu a systému prístupu k vhodným mechanizmom nápravy, ktoré vybavujú jednotlivcov v EHP prostriedkami na výkon ich práv a hľadanie nápravy bez toho, aby narazili na ťažkopádne prekážky správnych a súdnych prostriedkov nápravy, ktoré predstavujú kľúčové prvky, ktorými sa musí charakterizovať rámec ochrany údajov v súlade s európskym rámcom.

23. EDPB uznáva, že Spojené kráľovstvo z veľkej časti zohľadnilo príslušné ustanovenia všeobecného nariadenia o ochrane údajov vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov a v zákone o ochrane údajov z roku 2018; Európska komisia sa napriek tomu vyzýva, aby akýkoľvek vývoj v právnom rámci a praxi Spojeného kráľovstva, ktorý by mohol mať nepriaznivý vplyv na tieto oblasti, nepretržite monitorovala.

1.2.3. O prístupe orgánov verejnej moci k údajom prenášaným do Spojeného kráľovstva

24. EDPB berie na vedomie významné zmeny v právnom rámci Spojeného kráľovstva týkajúce sa bezpečnostných a spravodajských agentúr, najmä pokiaľ ide o zachytávanie a získavanie údajov o komunikácii. EDPB chápe, že tieto zmeny sú okrem iného reakciou na konanie začaté pred Súdnym dvorom EÚ a Európskym súdom pre ľudské práva a na ich nedávne rozsudky v tejto súvislosti.

25. EDPB víta najmä skutočnosť, že Spojené kráľovstvo zriadilo Investigatory Powers Tribunal (súd pre kontrolu vyšetrovacích právomocí, ďalej len „IPT“). IPT je nielen kompetentný rozhodovať o prípadoch použitia vyšetrovacích právomocí orgánmi presadzovania práva, ale aj spravodajskými službami. EDPB preto chápe, že IPT funguje ako príslušný súd v zmysle článku 47 Charty základných práv Európskej únie (ďalej len „Charta EÚ“).

26. EDPB ďalej pozitívne hodnotí zavedenie „komisárov pre justíciu“ [Judicial Commissioners] v zákone o vyšetrovacích právomociach z roku 2016 ako významné zlepšenie. Uvedomuje si, že dôležitou funkciou komisárov pre justíciu je schvaľovať *ex ante* v jednotlivých prípadoch rôzne opatrenia sledovania vrátane cieleného zachytávania a hromadného získavania údajov o komunikácii (takzvaný postup „dvojnásobného zabezpečenia“).

27. Na účely posúdenia účinnosti tejto dodatočnej úrovne dohľadu však EDPB vidí potrebu ďalšieho objasnenia scenárov, v prípade ktorých je možné zákonné zachytávanie bez schválenia komisárom pre vyšetrovacie právomoci [Investigatory Powers Commissioner] alebo komisármi pre justíciu, a vyzýva Európsku komisiu, aby ďalej posúdila a preukázala, že aj v prípadoch, keď sa postup dvojnásobného zabezpečenia neuplatňuje, právny rámec Spojeného kráľovstva poskytuje primerané záruky, a to aj prostredníctvom účinného *ex post* dohľadu a možností nápravy ponúkaných jednotlivcom, čím sa zabezpečí úroveň ochrany, ktorá je v podstate rovnocenná s úrovňou ochrany poskytovanej v rámci EÚ.

28. EDPB navyše vyzýva Európsku komisiu, aby ďalej posúdila podmienky, za ktorých sa možno odvolávať na naliehavé dôvody, a poskytla objasnenia týkajúce sa možných spôsobov výkonu práv dotknutých osôb a možných spôsobov nápravy, ktoré sa im ponúkajú v súvislosti s operáciami zasahovania do zariadení, najmä v prípade výnimky z postupu dvojnásobného zabezpečenia.

29. EDPB sa navyše domnieva, že je potrebné ďalšie objasnenie a posúdenie hromadných zachytávaní, najmä pokiaľ ide o výber a použitie selektorov, s cieľom objasniť, do akej miery prístup k osobným údajom spĺňa prahovú hodnotu stanovenú Súdnym dvorom EÚ, a aké záruky sú zavedené na ochranu

základných práv jednotlivcov, ktorých údaje sa v tejto súvislosti zachytávajú, vrátane tých, ktoré sa týkajú obdobia uchovávania údajov. Mimoriadne užitočné by bolo nezávislé posúdenie od príslušných orgánov dohľadu Spojeného kráľovstva. EDPB zároveň zdôrazňuje, že ešte o to dôležitejšie sa zdá, že „zahraničná komunikácia“, ktorá patrí do rozsahu postupov hromadného zachytávania, naznačuje, že Spojené kráľovstvo by mohlo údaje priamo hromadne zachytávať a získavať na území EÚ vrátane údajov v tranzite medzi EÚ a Spojeným kráľovstvom, čo by patrilo do rozsahu pôsobnosti návrhu rozhodnutia. EDPB vzhľadom na dôležitosť tohto aspektu vyzýva Európsku komisiu, aby pozorne sledovala vývoj v tejto súvislosti.

30. Pokiaľ ide o hromadné zachytávanie, EDPB zdôrazňuje dôsledné posúdenie zo strany Európskeho súdu pre ľudské práva a Súdneho dvora EÚ a pripomína obavy vyjadrené v súvislosti so sekundárnymi údajmi, pri ktorých by sa vzhľadom na ich citlivosť mali využívať osobitné záruky. EDPB preto vyzýva Európsku komisiu, aby starostlivo posúdila, či záruky stanovené v právnych predpisoch Spojeného kráľovstva pre takúto kategóriu osobných údajov zabezpečujú v podstate rovnocennú úroveň ochrany s ochranou zaručenou v EHP.

31. EDPB si v tejto súvislosti uvedomuje skutočnosť, že verejná správa Výboru pre spravodajstvo a bezpečnosť [Intelligence Security Committee] z roku 2016 o využívaní hromadných právomocí[13] sa týka postupov podľa predchádzajúceho právneho rámca, ktorý bol následne nahradený zákonom o vyšetrovacích právomociach z roku 2016. Napriek tomu považuje za potrebné ďalšie nezávislé posúdenie a dohľad nad používaním nástrojov automatizovaného spracúvania príslušnými dozornými orgánmi Spojeného kráľovstva a žiada Európsku komisiu, aby ďalej posúdila túto otázku a záruky, ktoré by sa v tejto súvislosti poskytli a/alebo mohli poskytnúť dotknutým osobám EHP.

32. EDPB súhlasí s názorom, ktorý vyjadril komisár pre vyšetrovacie právomoci, že je potrebné ďalšie preskúmanie a monitorovanie s cieľom zabezpečiť zachovanie a ďalšie zlepšovanie ochrany záruk, ktoré v praxi uplatňujú príslušné orgány v oblasti národnej bezpečnosti a spravodajských služieb na nápravu nesúladu s uplatňovaním príslušných právnych predpisov. EDPB víta aj skutočnosť, že komisár pre vyšetrovacie právomoci následne v roku 2019 uskutočnil preskúmanie svojho prístupu ku kontrole hromadného zachytávania, *„ktorá zahŕňala dôkladné preskúmanie technicky zložitých spôsobov, ktorými sa v skutočnosti hromadné zachytávanie realizuje“*, a zaviazal sa, že do kontrol hromadného zachytávania zahrnie od roku 2020 *„podrobné preskúmanie selektorov a vyhľadávacích kritérií, na ktoré poukázal Európsky súd pre ľudské práva“*. EDPB je vzhľadom na dôležitosť tohto aspektu znepokojený tým, že komisár pre vyšetrovacie právomoci ešte nevykonal podrobné preskúmanie selektorov a vyhľadávacích kritérií, a vyzýva Európsku komisiu, aby pozorne sledovala vývoj v tejto súvislosti, najmä preto, že konkrétny formát takéhoto dohľadu je ešte potrebné objasniť.

33. EDPB zdôrazňuje, že pokiaľ ide o poskytovanie údajov do zahraničia, výsledkom uplatňovania výnimky týkajúcej sa v záujme národnej bezpečnosti ustanovenej v právnych predpisoch Spojeného kráľovstva môže byť absencia záruk, ktoré zabezpečujú, aby sa dodržiavali aj zásady obmedzenia účelu, nevyhnutnosti a proporcionality, alebo v ktorých by sa predpokladalo, že dostatočné práva jednotlivcov, dohľad a náprava by sa poskytovali alebo dodržiavali aj v tretej krajine určenia. EDPB preto odporúča Európskej komisii, aby ďalej preskúmala celkové záruky stanovené v právnych predpisoch Spojeného kráľovstva, pokiaľ ide o poskytovanie údajov do zahraničia, najmä s ohľadom na uplatňovanie výnimiek týkajúcich sa v záujme národnej bezpečnosti.

[13] Pozri správa o preskúmaní rozsiahlych právomocí od nezávislého revízora právnych predpisov o terorizme, august 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

34. Napokon je EDPB znepokojený ďalšími formami výmeny informácií a poskytovania údajov na základe iných nástrojov, konkrétne rôznych medzinárodných dohôd, ktoré Spojené kráľovstvo uzatvorilo s inými tretími krajinami, najmä ak tieto nástroje zostávajú pre verejnosť neprístupné, ako napríklad Dohoda o komunikácii a spravodajstve medzi Spojeným kráľovstvom a USA. Účinok takejto dohody by mohol viesť k obchádzaniu záruk určených v súvislosti s prístupom a použitím osobných údajov a prístupe k nim na účely národnej bezpečnosti. EDPB sa domnieva, že uzatvorenie dvojstranných alebo mnohostranných dohôd s tretími krajinami na účely spravodajskej spolupráce, poskytnutie právneho základu pre priame zachytávanie a získavanie osobných údajov alebo prenos osobných údajov do týchto krajín môže takisto významne ovplyvniť podmienky ďalšieho použitia zhromaždených informácií, pretože tieto dohody môžu podľa posúdenia ovplyvniť právny rámec ochrany údajov Spojeného kráľovstva.

1.3. Záver

35. EDPB sa domnieva, že posúdenie primeranosti Spojeného kráľovstva je jedinečné z dôvodu predchádzajúceho postavenia Spojeného kráľovstva ako členského štátu EÚ. Okrem toho by to bolo zároveň prvé rozhodnutie o primeranosti zahŕňajúce doložku o ukončení platnosti [sunset clause].

36. EDPB preto uznáva mnoho oblastí konvergencie medzi rámcami ochrany údajov Spojeného kráľovstva a EÚ. Zároveň však po dôkladnej analýze návrhu rozhodnutia Európskej komisie a právnych predpisov Spojeného kráľovstva o ochrane údajov EDPB určil niekoľko výziev, ktoré sú v tomto stanovisku podrobne preskúmané. EDPB chce v tejto súvislosti zdôrazniť prvoradú úlohu Európskej komisie pri monitorovaní všetkého relevantného vývoja v Spojenom kráľovstve.

37. Vzhľadom na uvedené skutočnosti EDPB odporúča Európskej komisii, aby sa zaoberala výzvami, na ktoré sa poukazuje v tomto stanovisku. EDPB takisto vyzýva Európsku komisiu, aby pozorne sledovala všetok relevantný vývoj v Spojenom kráľovstve, ktorý môže mať vplyv na podstatnú rovnocennosť úrovne ochrany osobných údajov, a aby v prípade potreby prijala rýchle primerané opatrenia.

2. ÚVOD

2.1. Rámec ochrany údajov Spojeného kráľovstva

38. Rámec ochrany údajov Spojeného kráľovstva je vo veľkej miere založený na rámci ochrany údajov EÚ (najmä všeobecné nariadenie o ochrane údajov a smernica o presadzovaní práva EÚ), čo vyplýva z faktu, že Spojené kráľovstvo bolo do 31. januára 2020 členským štátom EÚ. V zákone Spojeného kráľovstva o ochrane údajov z roku 2018, ktorý nadobudol účinnosť 23. mája 2018 a ktorým sa zrušil zákon Spojeného kráľovstva o ochrane údajov z roku 1998, sa okrem transpozície smernice o presadzovaní práva EÚ ďalej uvádza uplatňovanie všeobecného nariadenia o ochrane údajov v právnych predpisoch Spojeného kráľovstva, ako aj udeľovanie právomocí a ukladanie povinností vnútroštátnemu dozornému orgánu pre ochranu údajov, Úradu komisára pre informácie Spojeného kráľovstva.

39. Ako je uvedené v odôvodnení 12 návrhu rozhodnutia Európskej komisie, vláda Spojeného kráľovstva uzákonila zákon o Európskej únii (vystúpenie) z roku 2018, ktorým sa do právnych predpisov Spojeného kráľovstva začleňujú priamo uplatniteľné právne predpisy EÚ. Podľa tohto zákona majú ministri Spojeného kráľovstva právomoc prostredníctvom zákonných nástrojov zaviesť sekundárne právne predpisy s cieľom vykonať potrebné úpravy právnych predpisov EÚ, ktoré boli ponechané po vystúpení Spojeného kráľovstva z EÚ, aby zodpovedali vnútroštátnym okolnostiam.

40. Príslušný právny rámec uplatniteľný v Spojenom kráľovstve po skončení prechodného obdobia [transition period][14] preto tvorí:

- všeobecné nariadenie Spojeného kráľovstva o ochrane údajov začlenené do práva Spojeného kráľovstva podľa zákona o vystúpení z Európskej únie z roku 2018, zmenené právnymi predpismi o ochrane údajov, súkromia a elektronických komunikáciách v dôsledku vystúpenia z EÚ z roku 2019,
- zákon o ochrane údajov z roku 2018, zmenený nariadeniami o ochrane údajov, súkromí a elektronických komunikáciách z roku 2019, a nariadenia o ochrane údajov, súkromí a elektronických komunikáciách (zmeny atď.) (vystúpenie z EÚ) z roku 2020 a
- zákon o vyšetrovacích právomociach z roku 2016.

(spolu ďalej len „rámec ochrany údajov Spojeného kráľovstva“).

2.2. Rozsah pôsobnosti posúdenia EDPB

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

42. Ako je uvedené v kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov: *„informácie poskytnuté Európskou komisiou by mali byť úplné a EDPB by mal mať možnosť vykonať vlastné posúdenie týkajúce sa úrovne ochrany údajov v tretej krajine“*[15].

43. V tejto súvislosti treba poznamenať, že EDPB dostal včas iba časť dokumentov relevantných pre preskúmanie právneho rámca Spojeného kráľovstva. Väčšinu právnych predpisov Spojeného kráľovstva, na ktoré sa odkazuje v návrhu rozhodnutia, získal EDPB prostredníctvom odkazov uvedených v návrhu. Európska komisia nemohla poskytnúť EDPB písomné vysvetlenia a záväzky od Spojeného kráľovstva súvisiace s výmenami medzi orgánmi Spojeného kráľovstva a Európskou komisiou, ktoré sú pre tento dokument relevantné[16].

[14] Prechodné obdobie je stanovené do 31. decembra 2020. Po tomto dátume sa právne predpisy EÚ už nevzťahujú na Spojené kráľovstvo. „Preklenovacie obdobie“ [bridge period] je stanovené najneskôr do 30. júna 2021 a označuje dodatočnú lehotu, počas ktorej sa poskytnutie osobných údajov z EÚ do Spojeného kráľovstva nepovažuje za prenos.
[15] Pozri WP254 rev.01, s. 3.
[16] So zreteľom na: článok 48 všeobecného nariadenia o ochrane údajov (poznámka pod čiarou č. 78 návrhu rozhodnutia); posilnené záruky a bezpečnostné opatrenia, ktoré uplatňujú prevádzkovatelia pri spracúvaní v kontexte národnej bezpečnosti (poznámka pod čiarou č. 64 návrhu rozhodnutia); požiadavku, aby prevádzkovateľ zvážil, či je potrebné odvolávať sa na výnimku v závislosti od konkrétneho prípadu, aj keď bolo vydané osvedčenie o národnej bezpečnosti (odôvodnenie 126 a poznámka pod čiarou č. 172 návrhu rozhodnutia); skutočnosť, že ochrana zastrešujúcej dohody medzi EÚ a USA sa bude vzťahovať na všetky osobné informácie vytvorené alebo uchované podľa dohody medzi Spojeným kráľovstvom a USA o zákone CLOUD, a to bez ohľadu na povahu alebo typ orgánu, ktorý podáva žiadosť, s ohľadom na konkrétne vykonávanie záruk v oblasti ochrany údajov, o ktorých sa stále rokuje medzi Spojeným kráľovstvom a USA, potvrdenie, že orgány Spojeného kráľovstva nechajú túto dohodu vstúpiť do platnosti, až keď sa presvedčia, že jej vykonávanie je v súlade s právnymi povinnosťami v nej stanovenými, vrátane jasnosti, pokiaľ ide o dodržiavanie súladu s normami ochrany údajov pre všetky údaje požadované podľa tejto dohody (odôvodnenie 153 návrhu rozhodnutia); situácie, keď sa údaje prenášajú z EÚ do Spojeného kráľovstva v rozsahu pôsobnosti tohto návrhu rozhodnutia, a skutočnosť, že vždy by existovalo „spojenie s Britskými

44. Vzhľadom na uvedené skutočnosti a obmedzený časový rámec (2 mesiace), ktorý mal EDPB k dispozícii na prijatie tohto stanoviska, sa Výbor rozhodol zamerať sa na niektoré konkrétne body uvedené v návrhu rozhodnutia a poskytnúť k nim vlastnú analýzu a stanovisko.

45. Pri analyzovaní právnych predpisov a postupov tretej krajiny, ktorá bola donedávna členským štátom EÚ, je zrejmé, že EDPB identifikoval mnoho aspektov ako v podstate rovnocenných. Vzhľadom na úlohu EDPB v procese prijatia záverov o primeranosti a množstvo právnych predpisov a postupov, ktoré bolo potrebné analyzovať, sa EDPB rozhodol sústrediť svoju pozornosť na tie aspekty, pri ktorých vnímal najväčšiu potrebu preskúmať ich podrobnejšie. Veľmi dôležitá časť analýzy okrem toho v súlade s judikatúrou Súdneho dvora EÚ pokrýva právny režim prístupu národnej bezpečnosti k osobným údajom prenášaným do Spojeného kráľovstva v záujme národnej bezpečnosti a prax aparátu národnej bezpečnosti v Spojenom kráľovstve. Treba však mať na pamäti, že národná bezpečnosť je zjavne oblasťou práva a praxe, kde právne predpisy členských štátov nie sú harmonizované na úrovni EÚ, a preto sa môžu líšiť.

46. EDPB zohľadnil platný európsky rámec ochrany údajov vrátane článkov 7, 8 a 47 Charty EÚ, ktorými sa chráni právo na súkromný a rodinný život, právo na ochranu osobných údajov a právo na účinný prostriedok nápravy a spravodlivý proces a článok 8 Európskeho dohovoru o ľudských právach (ďalej len „EDĽP"), ktorý chráni právo na súkromný a rodinný život. Okrem uvedených ustanovení EDPB zohľadnil aj požiadavky všeobecného nariadenia o ochrane údajov a relevantnú judikatúru.

47. Cieľom tejto činnosti je poskytnúť Európskej komisii stanovisko k posúdeniu primeranosti úrovne ochrany v Spojenom kráľovstve. Pojem „primeraná úroveň ochrany", ktorý existoval už podľa smernice 95/46/ES, Súdny dvor EÚ ďalej rozvinul. Je dôležité pripomenúť normu stanovenú Súdnym dvorom v rozsudku Schrems I, a to že – zatiaľ čo „úroveň ochrany" v tretej krajine musí byť „v podstate rovnocenná" úrovni ochrany zaručenej v EÚ – *„prostriedky, ktoré v tomto ohľade použije táto tretia krajina na zabezpečenie takejto úrovne ochrany, môžu byť rozdielne od tých, ktoré sa zaviedli v rámci Únie"*[17]. Cieľom preto nie je odzrkadľovať každý jeden bod európskych právnych predpisov, ale stanoviť základné prvky a hlavné požiadavky preskúmavaných právnych predpisov. Primeranosť možno dosiahnuť kombináciou práv dotknutých osôb a povinností tých, ktorí spracúvajú údaje alebo vykonávajú kontrolu nad takýmto spracúvaním, a dohľadom zo strany nezávislých orgánov. Pravidlá ochrany údajov sú však účinné len vtedy, ak sú vymožiteľné a v praxi sa dodržiavajú. Preto je potrebné zvážiť nielen obsah pravidiel týkajúcich sa osobných údajov prenášaných do tretej krajiny alebo medzinárodnej organizácii, ale aj systém zavedený na zabezpečenie účinnosti takýchto pravidiel. Účinné mechanizmy presadzovania sú mimoriadne dôležité pre účinnosť pravidiel ochrany údajov[18].

ostrovmi" a akékoľvek zasahovanie do zariadení pokrývajúce tieto údaje by preto podliehalo požiadavke povinného príkazu v § 13 ods. 1 zákona o vyšetrovacích právomociach z roku 2016 (odôvodnenie 206 návrhu rozhodnutia) a poskytnuté príklady operačných účelov (odôvodnenie 216 a poznámka pod čiarou č. 369 návrhu rozhodnutia).

[17] Pozri rozsudok Súdneho dvora vo veci C-362/14, Maximillian Schrems/Data Protection Commissioner, 6. októbra 2015, ECLI:EU:C:2015:650 (ďalej len „Schrems I"), body 73 – 74.

[18] Pozri WP254 rev.01, s. 2.

2.3. Všeobecné pripomienky a obavy

2.3.1. Medzinárodné záväzky prijaté Spojeným kráľovstvom

48. Podľa článku 45 ods. 2 písm. c) všeobecného nariadenia o ochrane údajov a kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov[19] musí Európska komisia pri posudzovaní primeranosti úrovne ochrany v tretej krajine zohľadňovať aj medzinárodné záväzky, ktoré dotknutá krajina prevzala, alebo iné záväzky vyplývajúce z účasti tretej krajiny na viacstranných alebo regionálnych systémoch, najmä vo vzťahu k ochrane osobných údajov, ako aj plnenie týchto povinností. Okrem toho by sa malo zohľadniť pristúpenie tretej krajiny k Dohovoru Rady Európy z 28. januára 1981 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (ďalej len „Dohovor č. 108“)[20] a dodatkovému protokolu k nemu[21].

49. **EDPB v tejto súvislosti víta skutočnosť, že Spojené kráľovstvo pristúpilo k EDĽP a patrí pod jurisdikciu Európskeho súdu pre ľudské práva. Okrem toho Spojené kráľovstvo dodržiava aj Dohovor č. 108 a dodatkový protokol k nemu, v roku 2018 podpísalo Dohovor č. 108+[22] a v súčasnosti pracuje na jeho ratifikácii.**

2.3.2. Možné budúce odchýlky od rámca ochrany údajov Spojeného kráľovstva

50. Podľa odôvodnenia 281 návrhu rozhodnutia musí Európska komisia zohľadniť, že s koncom prechodného obdobia stanoveného v dohode o vystúpení[23] Spojené kráľovstvo spravuje, uplatňuje a presadzuje svoj vlastný režim ochrany údajov a ihneď po ukončení platnosti ustanovenia o preklenovacom období podľa článku FINPROV.10A Dohody o obchode a spolupráci medzi EÚ a Spojeným kráľovstvom[24] to môže zahŕňať najmä úpravy alebo zmeny v rámci ochrany údajov, ktoré sa posudzujú v návrhu rozhodnutia, ako aj ďalší relevantný vývoj.

51. Európska komisia sa preto rozhodla do svojho návrhu rozhodnutia zahrnúť doložku o ukončení platnosti[25], ktorou sa stanovuje dátum skončenia platnosti na štyri roky odo dňa nadobudnutia účinnosti.

52. Je dôležité poznamenať, že možnosť ministrov Spojeného kráľovstva po skončení preklenovacieho obdobia zavádzať sekundárne právne predpisy môže v budúcnosti viesť k značnej odchýlke rámca ochrany údajov Spojeného kráľovstva od rámca ochrany údajov EÚ.

53. Vláda Spojeného kráľovstva skutočne naznačila svoj zámer vypracovať samostatné a nezávislé politiky v oblasti ochrany údajov, ktoré by potom mohli viesť k odchýlkam od právnych predpisov EÚ o ochrane údajov[26]. Súčasťou tohto zámeru je zahrnutie aspektov osobných údajov do obchodných

[19] Pozri WP254 rev.01, s. 2.
[20] Pozri Dohovor o ochrane jednotlivcov pri spracovaní osobných údajov, Dohovor č. 108, 28. január 1981.
[21] Pozri Dodatkový protokol k Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov týkajúci sa orgánov dozoru a cezhraničných tokov údajov, otvorený na podpis 8. novembra 2001.
[22] Pozri protokol, ktorým sa mení Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (ďalej len „Dohovor 108+“) z 18. mája 2018.
[23] Pozri Dohodu o vystúpení Spojeného kráľovstva Veľkej Británie a Severného Írska z Európskej únie a z Európskeho spoločenstva pre atómovú energiu (Ú. v. EÚ L 029, 31.1.2020, s. 7).
[24] Pozri Dohodu o obchode a spolupráci medzi Európskou úniou a Európskym spoločenstvom pre atómovú energiu na jednej strane a Spojeným kráľovstvom Veľkej Británie a Severného Írska na strane druhej (Ú. v. EÚ L 444, 31.12.2020, s. 14).
[25] Pozri článok 4 návrhu rozhodnutia. Pozri aj odôvodnenie 282 návrhu rozhodnutia.
[26] Národná stratégia Spojeného kráľovstva v oblasti údajov (naposledy aktualizovaná 9. decembra 2020), https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) obsahuje ako jednu zo svojich misií: *„Presadzovanie medzinárodného toku údajov. Tok informácií cez hranice podporuje globálne*

dohôd[27], čo je postup, ktorý so sebou prináša riziko zníženia úrovne ochrany osobných údajov poskytovanej v Spojenom kráľovstve[28].

54. Napokon po skončení prechodného obdobia už Spojené kráľovstvo nie je viazané nielen judikatúrou Súdneho dvora, ale ani už prijaté rozsudky Súdneho dvora, ktoré sa v právnom rámci Spojeného kráľovstva považujú za ponechanú judikatúru, už nemusia byť pre Spojené kráľovstvo záväzné, keďže Spojené kráľovstvo má po skončení preklenovacieho obdobia konkrétne možnosť zmeniť ponechané právne predpisy EÚ a jeho najvyšší súd už nie je viazaný žiadnou ponechanou judikatúrou EÚ[29].

55. **Vzhľadom na riziká súvisiace s možným odchýlením rámca ochrany údajov Spojeného kráľovstva od *acquis* EÚ po skončení preklenovacieho obdobia EDPB víta rozhodnutie Európskej komisie začleniť do návrhu rozhodnutia doložku o ukončení platnosti s dĺžkou trvania štyri roky. EDPB by však na tomto mieste chcel zdôrazniť význam monitorovacej úlohy Európskej komisie[30]. Európska komisia by mala monitorovať všetky relevantné zmeny v Spojenom kráľovstve, ktoré môžu mať vplyv na podstatnú rovnocennosť úrovne ochrany osobných údajov, ktoré sa priebežne a trvale prenášajú na základe rozhodnutia o primeranosti v Spojenom kráľovstve od nadobudnutia jeho účinnosti. Európska komisia by okrem toho mala podľa konkrétnych okolností prijať primerané opatrenie v podobe pozastavenia, zmeny alebo zrušenia rozhodnutia o primeranosti, ak po jeho prijatí získa informácie, že v Spojenom kráľovstve už nie je zabezpečená primeraná úroveň ochrany.**

56. EDPB zo svojej strany vynaloží všetko úsilie na to, aby informoval Európsku komisiu o akýchkoľvek príslušných opatreniach, ktoré prijali dozorné orgány pre ochranu údajov členského štátu (ďalej len „dozorné orgány“) v komerčnom alebo verejnom sektore, najmä pokiaľ ide o sťažnosti podané dotknutými osobami v EHP týkajúce sa prenosu osobných údajov z EHP do Spojeného kráľovstva.

---

obchodné operácie, dodávateľské reťazce a obchod a podporuje rast na celom svete. Zohráva aj širšiu spoločenskú úlohu. Prenos osobných údajov zaisťuje, že ľudia budú mať zaplatené platy, a pomáha im na diaľku komunikovať s blízkymi. A ako pandémia koronavírusu preukázala, výmena údajov týkajúcich sa zdravia môže pomôcť pri dôležitom vedeckom výskume chorôb a zároveň zjednotiť krajiny v reakcii na globálne núdzové situácie týkajúce sa zdravia. ***Po vystúpení z Európskej únie bude Spojené kráľovstvo presadzovať prínosy, ktoré môžu údaje priniesť.*** *Budeme presadzovať domáce osvedčené postupy a spolupracovať s medzinárodnými partnermi,* ***aby sme zabezpečili, že údaje nebudú neprimerane obmedzovať národné hranice a rozdrobené regulačné režimy****, aby bolo možné plne využiť ich potenciál.“* (zdôraznenie doplnené).

[27] Tamže: *„Uľahčenie cezhraničných tokov údajov:* ***Budeme pracovať na celosvetovej úrovni na odstránení zbytočných prekážok medzinárodných tokov údajov. Pri našich obchodných rokovaniach sa dohodneme na ambicióznych ustanoveniach o údajoch*** *a využijeme naše nové nezávislé miesto vo Svetovej obchodnej organizácii na ovplyvňovanie lepších obchodných pravidiel týkajúcich sa údajov.* ***Odstránime prekážky medzinárodných prenosov údajov****, ktoré podporujú rast a inovácie, a to aj vytvorením novej spôsobilosti Spojeného kráľovstva, ktorá prináša nové a inovatívne mechanizmy určené pre medzinárodný prenos údajov. Budeme takisto spolupracovať s partnermi v rámci skupiny G20 na vytvorení interoperability medzi národnými režimami údajov s cieľom minimalizovať nesúlad pri prenose údajov medzi rôznymi krajinami“.* (zdôraznenie doplnené).

[28] Pozri uznesenie Európskeho parlamentu z 12. decembra 2017 „Smerom k stratégii digitálneho obchodu“ [2017/2065 (INI)], oddiel V, v ktorom zdôraznil, že *„o ochrane osobných údajov sa v obchodných dohodách [EÚ] nedá vyjednávať“*, dostupné na adrese: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_SK.pdf. Pozri aj uznesenie Európskeho parlamentu z 25. marca 2021 o hodnotiacej správe Komisie o vykonávaní všeobecného nariadenia o ochrane údajov po dvoch rokoch jeho uplatňovania, ods. 28, v ktorom sa uvádza: *“podporuje prax Komisie zaoberať sa ochranou údajov a tokmi osobných údajov oddelene od obchodných dohôd”*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_SK.html.

[29] Pozri § 6 ods. 3 až 6 zákona o vystúpení z EÚ z roku 2018.

[30] Pozri článok 45 ods. 4 všeobecného nariadenia o ochrane údajov.

3. VŠEOBECNÉ ASPEKTY OCHRANY ÚDAJOV

3.1. Zásady obsahu

57. Kapitola 3 kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov je venovaná „Zásadám obsahu“. Systém tretej krajiny ich musí obsahovať, aby sa jej úroveň ochrany údajov mohla považovať za takú, ktorá je v zásade rovnocenná s úrovňou zaručenou v EÚ. EDPB uznáva skutočnosť, že Spojené kráľovstvo nemá kodifikovanú ústavu v tom zmysle, že neexistuje jediný dokument, ktorý by upravoval jeho základné pravidlá. Právo na rešpektovanie súkromného a rodinného života (a právo na ochranu údajov ako súčasť tohto práva) a právo na spravodlivý proces[31] sú však zahrnuté v zákone o ľudských právach z roku 1998 a ústavnú hodnotu tohto právneho predpisu uznali súdy Spojeného kráľovstva. Zákon o ľudských právach z roku 1998 skutočne začleňuje práva obsiahnuté v EDĽP[32]. V zákone o ľudských právach z roku 1998 sa navyše s veľkým dôrazom uvádza, že akýkoľvek postup orgánov verejnej moci musí byť zlučiteľný s EDĽP[33].

58. EDPB okrem štrukturálnych a formalistických rozdielov medzi právnymi predpismi Spojeného kráľovstva a EÚ poznamenáva, ako sa dá očakávať, že prístup Spojeného kráľovstva k ochrane údajov je podobný prístupu v EÚ, ktorý vyplýva zo skutočnosti, že Spojené kráľovstvo bolo členským štátom EÚ do 31. januára 2020. V dôsledku toho je veľa zásad obsahu zosúladených so zásadami obsahu vo všeobecnom nariadení o ochrane údajov; preto poskytujú úroveň ochrany v podstate rovnocennú s úrovňou poskytovanou EÚ. EDPB sa rozhodol, že nebude ďalej rozvíjať analýzu tých zásad obsahu, ktoré sú v súlade s právnymi predpismi EÚ, a s analýzou, ktorú poskytla Európska komisia vo svojom návrhu rozhodnutia, je spokojný. Ide napríklad o tieto zásady obsahu: pojmy (napr. „osobné údaje“, „spracúvanie osobných údajov“, „prevádzkovateľ“), dôvody zákonného a spravodlivého spracúvania na legitímne účely, obmedzenie účelu, kvalita a primeranosť údajov, uchovávanie, bezpečnosť a dôvernosť údajov, transparentnosť, osobitné kategórie údajov, priamy marketing, automatizované rozhodovanie a profilovanie. EDPB ďalej poznamenáva, že všeobecné nariadenie Spojeného kráľovstva o ochrane údajov a zákon o ochrane údajov z roku 2018 zahŕňajú zásady obsahu, ktoré idú nad rámec toho, čo sa požaduje v kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov, a sú v nich zahrnuté zásady obsiahnuté vo všeobecnom nariadení o ochrane údajov; zvyšujú teda úroveň ochrany stanovenú v Spojenom kráľovstve. K takýmto zásadám obsahu patria napríklad tie, ktoré sa týkajú oznámení o porušení ochrany osobných údajov, zodpovednej osoby, posúdenia vplyvu na ochranu údajov a špecificky navrhnutej a štandardnej ochrany údajov.

59. Ako sa však uvádza v úvode, EDPB by sa chcel v tomto stanovisku osobitne zaoberať niektorými bodmi, v súvislosti s ktorými má obavy, a od Európskej komisie požaduje objasnenie.

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

60. Takzvaná „imigračná výnimka“ stanovená v časti 1 ods. 4 **prílohy 2 k zákonu o ochrane údajov z roku 2018** umožňuje prevádzkovateľom zapojeným do „kontroly prisťahovalectva“ neuplatňovať určité práva dotknutých osôb stanovené v zákone o ochrane údajov z roku 2018, ak by sa tým pravdepodobne „*dotýkalo zachovanie účinnej kontroly prisťahovalectva*“ alebo „*vyšetrovanie alebo odhaľovanie činností, ktoré by ohrozovali udržiavanie účinnej kontroly prisťahovalectva*“.

[31] Pozri články 6 a 8 EDĽP (príloha 1 k zákonu o ľudských právach z roku 1998).
[32] Ďalšie informácie sú uvedené v odôvodneniach 8 až 10 návrhu rozhodnutia.
[33] Pozri § 6 zákona o ľudských právach z roku 1998.

61. Ako uznala Európska komisia vo svojom návrhu rozhodnutia[34] a ako sa uvádza v stanovisku výboru LIBE Európskeho parlamentu k uzavretiu Dohody o obchode a spolupráci medzi EÚ a Spojeným kráľovstvom v mene EÚ[35], táto výnimka je **formulovaná „všeobecne“**. Vzťahuje sa na tieto práva: právo na informácie, právo na prístup, právo na vymazanie, právo na obmedzenie spracúvania a právo namietať.

62. Okrem toho je dôležité poznamenať, že táto výnimka sa takisto uplatňuje v prípade, ak osobné údaje nezhromažďuje na účely kontroly prisťahovalectva prevádzkovateľ (ďalej len „prevádzkovateľ 1“), ale tento ich sprístupňuje ďalšiemu prevádzkovateľovi (ďalej len „prevádzkovateľ 2“), ktorý tieto osobné údaje spracúva na účely kontroly prisťahovalectva (napr. Ministerstvo vnútra Spojeného kráľovstva)[36].

63. Vo veci *Open Rights Group & Anor, R (O uplatňovaní)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (3. októbra 2019)* žalobcovia spochybnili zákonnosť imigračnej výnimky z dôvodu, že to bolo v rozpore s článkom 23 všeobecného nariadenia o ochrane údajov a nezlučiteľné s právami zaručenými v článkoch 7 a 8 Charty EÚ týkajúcich sa súkromia a ochrany osobných údajov. High Court of England and Wales (ďalej len „Vrchný súd“) posúdil, či je imigračná výnimka uvedená v časti 1 ods. 4 prílohy 2 k zákonu o ochrane údajov z roku 2018 zákonná, a dospel k záveru v prospech jej zákonnosti.

---

[34] Pozri odôvodnenia 62 až 65 návrhu rozhodnutia.

[35] V tejto súvislosti, pokiaľ ide o **všeobecnú formuláciu** imigračnej výnimky, pozri stanovisko Výboru pre občianske slobody, spravodlivosť a vnútorné veci k uzavretiu Dohody o obchode a spolupráci medzi Európskou úniou a Európskym spoločenstvom pre atómovú energiu na jednej strane a Spojeným kráľovstvom Veľkej Británie a Severného Írska na strane druhej a Dohody medzi Európskou úniou a Spojeným kráľovstvom Veľkej Británie a Severného Írska o bezpečnostných postupoch pri výmene a ochrane utajovaných skutočností [2020/0382(NLE)], 5. februára 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_SK.pdf, ods. 10: *„v tejto súvislosti pripomína uznesenia Parlamentu z februára a júna 2020, ktoré poukazujú na **všeobecnú a rozsiahlu výnimku** zo spracúvania osobných údajov na účely prisťahovalectva podľa zákona Spojeného kráľovstva o ochrane údajov“ a* ods. 11: *„domnieva sa, že je potrebné zmeniť **všeobecnú a rozsiahlu** výnimku zo spracúvania osobných údajov na účely prisťahovalectva podľa zákona Spojeného kráľovstva o ochrane údajov […] predtým, ako bude možné prijať platné rozhodnutie o primeranosti;”* (zdôraznenie doplnené).

[36] Pozri príklad uvedený v dokumente od ICO „Usmernenia k všeobecnému nariadeniu o ochrane údajov (GDPR)“, v. 1. januára 2021, s. 307 (zdôraznenie doplnené): *„Súkromná organizácia (prevádzkovateľ 1) upozorní ministerstvo vnútra (prevádzkovateľ 2) na zamestnanca, o ktorom sa predpokladá, že na preukázanie svojej totožnosti predložil falošné dokumenty a kvalifikácie na získanie zamestnania. Zamestnávateľ poskytne ministerstvu vnútra príslušné informácie. Právo jednotlivca byť informovaný o tom, že jeho osobné údaje boli postúpené ministerstvu vnútra, je obmedzené, pokiaľ by jeho uplatnenie mohlo ovplyvniť vyšetrovanie.*
***Zamestnávateľ preto nie je povinný informovať jednotlivca o tom, že jeho informácie boli postúpené ministerstvu vnútra**, a **ministerstvo vnútra** naopak nie je povinné poskytnúť jednotlivcovi oznámenie o ochrane osobných údajov, v ktorom ho informuje, že teraz spracúva jeho osobné údaje. Výnimka sa vzťahuje na oboch prevádzkovateľov v rovnakom rozsahu.*
*Zamestnanec však žiada kópiu jeho osobných údajov od ministerstva vnútra, ktoré ich teraz vyšetruje. **Ministerstvo vnútra sa môže odvolať na výnimku** s cieľom zadržať časť jeho údajov, ak by ich poskytnutie mohlo ovplyvniť vyšetrovanie. Ak by zamestnanec podal podobnú žiadosť **svojmu zamestnávateľovi, ten by si takisto mohol uplatniť výnimku** v rovnakom rozsahu.“*
Inými slovami, ako je objasnené na s. 300: *„Vo väčšine prípadov bude prevádzkovateľom, ktorý si uplatňuje túto výnimku, ministerstvo vnútra alebo niektorá z jeho agentúr a dodávateľov. Je však dôležité poznamenať, že uplatňovanie tejto výnimky sa neobmedzuje iba na ministerstvo vnútra. Môže byť relevantná aj pre iných prevádzkovateľov, ako sú zamestnávatelia, univerzity a polícia, ktorí sú v otázkach prisťahovalectva v kontakte s ministerstvom vnútra.“*

64. Vrchný súd zastával predovšetkým názor, že:

- *„[…] Imigračná výnimka je zjavne záležitosťou ‚dôležitého verejného záujmu' a sleduje legitímny cieľ.[…]"*, bod 30;
- *„Imigračná výnimka spĺňa požiadavky na to, aby bolo opatrenie ‚v súlade so zákonom. […]'"*, bod 38;
- *„Na imigračnú výnimku sa možno odvolať iba ak a v takom rozsahu, v akom **by bolo** súladom s ‚uvedenými ustanoveniami GDPR' **pravdepodobne dotknuté** zachovanie účinnej kontroly prisťahovalectva alebo vyšetrovanie alebo odhaľovanie činností, ktoré by ohrozovali udržiavanie účinnej kontroly prisťahovalectva. Slová ‚by bolo pravdepodobne dotknuté' v kontexte zákona o ochrane údajov z roku 1998 (ktorý predchádzal zákonu o ochrane údajov z roku 2018) boli vykladané tak, že znamenajú ‚veľmi významnú a závažnú šancu na poškodenie konkrétneho verejného záujmu. Miera rizika musí byť taká, aby ‚mohlo výrazne' dôjsť k poškodeniu týchto záujmov, a to aj v prípade, že riziko má ďaleko od toho, aby bolo skôr pravdepodobné ako nie […]."*, bod 39 (zdôraznenie doplnené).

65. Treba poznamenať, že tento rozsudok nie je podľa vedomostí EDPB konečný a bolo proti nemu podané odvolanie.

66. Ako je uvedené v usmerneniach EDPB k obmedzeniam podľa článku 23 všeobecného nariadenia o ochrane údajov (ďalej len „usmernenia k článku 23 všeobecného nariadenia o ochrane údajov")[37] *„[…] v kontexte všeobecného nariadenia o ochrane údajov sa obmedzenia ustanovujú v **legislatívnom opatrení**, týkajú sa **obmedzeného počtu práv dotknutých osôb a/alebo povinností prevádzkovateľov**, ktoré sú uvedené v článku 23 všeobecného nariadenia o ochrane údajov, **rešpektujú podstatu** dotknutých základných práv a slobôd, predstavujú **potrebné a primerané opatrenie** v demokratickej spoločnosti a chránia jeden z dôvodov uvedených v článku 23 ods. 1 všeobecného nariadenia o ochrane údajov […]".*[38]

67. EDPB zároveň pripomína, že v odôvodnení 41 všeobecného nariadenia o ochrane údajov sa uvádza, že *„keď sa v tomto nariadení odkazuje na **právny základ alebo legislatívne opatrenie**, nemusí sa tým nevyhnutne vyžadovať legislatívny akt prijatý parlamentom, bez toho, aby boli dotknuté požiadavky vyplývajúce z ústavného poriadku dotknutého členského štátu. Takýto právny základ alebo legislatívne opatrenie by však mali byť **jasné a presné a ich uplatňovanie by malo byť predvídateľné pre tie osoby, na ktoré sa vzťahujú**, a to v súlade s judikatúrou Súdneho dvora Európskej únie […] a Európskeho súdu pre ľudské práva"* (zdôraznenie doplnené).

68. Aj keď Európsky súd pre ľudské práva spresnil, že *„pokiaľ ide o slová „v súlade so zákonom [law]" a „ustanovené zákonom [law]", ktoré sú uvedené v článkoch 8 až 11 dohovoru, [EDĽP] poznamenáva, že pojmu „zákon [law]" vždy rozumel v jeho „hmotnoprávnom" zmysle, nie vo „formálnom" zmysle; zahŕňa jednak ‚písané právo', ktoré obsahuje tak podzákonné predpisy, ako aj vykonávacie predpisy prijaté stavovskou komorou na základe právomoci prenesenej na ňu zákonodarcom v rámci jej nezávislej normotvornej právomoci, ako aj ‚nepísané právo'. ‚Zákon' [law[treba chápať tak, že zahŕňa tak písaný text, ako aj **‚právo tvorené súdmi'"**[39], v usmerneniach k článku 23 všeobecného nariadenia o ochrane údajov sa pripomína, že *„podľa judikatúry Súdneho dvora EÚ musí každé **legislatívne***

[37] Pozri usmernenia EDPB 10/2020 o obmedzeniach podľa článku 23 všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 15. decembra 2020, ktoré sa v súčasnosti dokončujú po verejnej konzultácii, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

[38] Pozri usmernenia k článku 23 všeobecného nariadenia o ochrane údajov, ods. 9, s. 5.

[39] Pozri Európsky súd pre ľudské práva, Sanoma Uitgevers B.V./Holandské kráľovstvo, 14. septembra 2010, EC:ECHR:2010:0914JUD003822403, ods. 83 (zdôraznenie doplnené).

opatrenie *prijaté na základe článku 23 ods. 1 všeobecného nariadenia o ochrane údajov predovšetkým* ***spĺňať konkrétne požiadavky stanovené v článku 23 ods. 2 všeobecného nariadenia o ochrane údajov****. V článku 23 ods. 2 všeobecného nariadenia o ochrane údajov sa uvádza, že legislatívne opatrenia, ktorými sa ukladajú obmedzenia práv dotknutých osôb a povinnosti prevádzkovateľov, obsahujú tam, kde je to relevantné,* ***konkrétne ustanovenia o niekoľkých kritériách uvedených ďalej****. Všetky požiadavky uvedené ďalej* ***by mali byť*** *spravidla* ***zahrnuté v legislatívnom opatrení****, ktorým sa ukladajú obmedzenia podľa článku 23 všeobecného nariadenia o ochrane údajov.“*[40]

69. V tejto súvislosti možno poznamenať, že v samotnej **imigračnej výnimke sa nešpecifikujú nasledujúce prvky uvedené v článku 23 ods. 2 všeobecného nariadenia o ochrane údajov**:

- „záruky zabraňujúce zneužitiu údajov alebo nezákonnému prístupu či prenosu“ [písm. d)];
- „prevádzkovateľ alebo kategórie prevádzkovateľov [písm. e)][41];
- „riziká pre práva a slobody dotknutých osôb“ [písm. g)];
- „práva dotknutých osôb na informovanie o obmedzení, pokiaľ tým nie je ohrozený účel obmedzenia“ [písm. h)].

70. V dokumente „Usmernenia k všeobecnému nariadeniu o ochrane údajov (GDPR)“ od ICO[42], ktorý obsahuje kapitolu o „imigračnej výnimke“, je uvedené objasnenie imigračnej výnimky, **nemôže** však sám osebe obsahovať záväzné pravidlá, ktoré by ju dopĺňali. Otázka „kvality zákona“ [law] je navyše osobitne dôležitá vzhľadom na význam obmedzených práv a rozšírenie výnimky[43].

---

[40] Pozri usmernenia k článku 23 všeobecného nariadenia o ochrane údajov, ods. 45 a 46, s. 11. Podľa článku 52 ods. 3 Charty EÚ *„V rozsahu, v akom táto charta obsahuje práva, ktoré zodpovedajú právam zaručeným v Európskom dohovore o ochrane ľudských práv a základných slobôd, zmysel a rozsah týchto práv je rovnaký ako zmysel a rozsah práv ustanovených v uvedenom dohovore. Toto ustanovenie nebráni tomu, aby právo Únie priznávalo širší rozsah ochrany týchto práv“.* Pokiaľ ide o pojem **„ktoré ustanovuje zákon“ [**law] podľa článku 52 ods. 1 Charty EÚ, mali by sa použiť kritériá vypracované Európskym súdom pre ľudské práva tak, ako sa to navrhuje v niekoľkých návrhoch generálneho advokáta Súdneho dvora EÚ, pozri napríklad návrhy v spojených veciach C-203/15 a C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, bod 137 až 154 a vo veci C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, bod 88 až 114. Preto možno uviesť odkaz okrem iného na rozsudok Európskeho súdu pre ľudské práva vo veci Weber a Saravia v. /Nemecko, bod 84: *„Súd opätovne konštatuje, že výraz „**v súlade so zákonom**“ [law] v zmysle článku 8 ods. 2 [EDĽP] vyžaduje po prvé to, aby napadnuté opatrenie malo určitý základ vo **vnútroštátnom práve** [law]; odkazuje aj na **kvalitu** predmetného **zákona** [law] a vyžaduje, aby bol prístupný pre dotknutú osobu, ktorá musí byť okrem toho schopná predvídať jeho dôsledky pre ňu, a v súlade s právnym štátom.“* (zdôraznenie doplnené).
Pozri aj odôvodnenie 41 všeobecného nariadenia o ochrane údajov: *„Takýto [právny základ alebo] legislatívne opatrenie by však mali byť **jasné a presné a** ich uplatňovanie by malo byť **predvídateľné pre tie osoby, na ktoré sa vzťahujú**, a to v súlade s judikatúrou Súdneho dvora Európskej únie [...] a Európskeho súdu pre ľudské práva“* (zdôraznenie doplnené).

[41] Pozri vyššie uvedenú vec Vrchného súdu, bod 54: *"Podľa môjho názoru nie je nič nezákonné na tom, že imigračná výnimka je k dispozícii **všetkým prevádzkovateľom údajov**, ktorí spracúvajú údaje na konkrétne účely.“ Ako uvádzajú odporcovia, bez odseku 4 pododsekov 3 až 4 by sa imigračná výnimka stala neúčinnou v prípadoch, keď sa údaje získavajú od tretích strán (napríklad od miestneho orgánu alebo Daňového a colného úradu Jej Veličenstva) na účely zachovania účinnej kontroly prisťahovalectva.“* (zdôraznenie doplnené), teda potvrdzuje **všeobecné** uplatňovanie obmedzení.

[42] „Usmernenia k všeobecnému nariadeniu o ochrane údajov (GDPR)“ od ICO, v. 1. januára 2021, s. 299 – 307.

[43] Pozri bod 57 vyššie uvedenej veci Vrchného súdu: *„Pán Knight ma informuje, že komisár dokončuje usmernenie o výnimke, ale „zákonný“ status bude mať iba v tom zmysle, že bude vydané na základe právomocí komisára podľa článku 57 ods. 1 GDPR. Podľa zákona o ochrane údajov z roku 2018 nebude mať právne postavenie* [statutory status]*.“*

71. *A fortiori* sa v „teste škody“ [prejudice test] nestanovujú záruky zabraňujúce zneužitiu údajov alebo nezákonnému prístupu či prenosu, ktoré by malo implementovať napríklad ministerstvo vnútra.

72. Na základe všetkých vyššie uvedených skutočností EDPB poznamenáva, že sú potrebné ďalšie objasnenia týkajúce sa uplatňovania imigračnej výnimky.

73. EDPB ďalej upozorňuje na neexistenciu právne záväzného nástroja, ktorý by objasňoval imigračnú výnimku s cieľom posúdiť, či je v podstate rovnocenná s článkom 23 všeobecného nariadenia o ochrane údajov a článkami 7 a 8 Charty EÚ. EDPB sa zároveň domnieva, že nevyhnutnosť a proporcionalitu širokého rozsahu osobnej pôsobnosti a imigračnej výnimky musí Európska komisia ďalej preukázať aj s podporou dôkazov.

74. **EDPB napokon vyzýva Európsku komisiu, aby overila súčasný stav konania *Open Rights Group & Anor, R (O uplatňovaní)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* uvedeného vyššie a, keďže tento rozsudok nie je právoplatný (prekážka rozhodnutej veci), aby overila, či je potvrdený alebo preskúmaný napadnutým rozsudkom, zohľadnila každú aktualizáciu v tejto súvislosti a uviedla ju v rozhodnutí o primeranosti. EDPB takisto vyzýva**

Odôvodnenie zavedenia právne záväzného usmernenia, ktoré podporuje ICO, sa uvádza najmä v bodoch 56 až 60 rozsudku:
„56. Na záver chcem upriamiť pozornosť na závery komisára, že bez sprievodného zákonného usmernenia, ktoré by poskytovalo záruky týkajúce sa významu a uplatňovania imigračnej výnimky, by výnimka nepredstavovala primerané vykonávanie článku 23 ods. 1 GDPR. Pán Knight hovorí, že ustanovenie doplnené o takéto usmernenie je primerané.
57. Pán Knight ma informuje, že komisár dokončuje usmernenie o výnimke, ale „zákonný“ status bude mať iba v tom zmysle, že bude vydané na základe právomocí komisára podľa článku 57 ods. 1 GDPR. Podľa zákona o ochrane údajov z roku 2018 nebude mať právne postavenie. Treba takisto uviesť, že ministerstvo vnútra pripravilo návrh interných usmernení pre zamestnancov o imigračnej výnimke [pozri vyššie bod 22]. V praxi má usmernenie vydané komisárom vplyv bez ohľadu na jeho právny základ. Komisár však nemá žiadne oprávnenie vydávať „záväzné“ usmernenie takého druhu, aký mal Najvyšší súd na mysli vo veci Christian Institute (body 101 a 107). Zdá sa, že primárne právo by bolo potrebné, ak by sa považovalo za nevyhnutné, aby existovalo usmernenie týkajúce sa imigračnej výnimky rovnakej povahy ako kódexy postupov, ktoré sú v súčasnosti stanovené v § 121 – 124 zákona o ochrane údajov z roku 2018.
58. Pán Knight vo svojom argumente za zákonné usmernenie tvrdí, že kontext, v ktorom dôjde k použitiu imigračnej výnimky, nevyhnutne súvisí s obavami o nevyhnutnosť a proporcionalitu jej existencie a použitia. Upozorňuje na dve veci, predovšetkým v právnom kontexte. Po prvé, je pravdepodobné, že osobné údaje, na ktoré sa vzťahuje imigračná výnimka, budú zahŕňať údaje osobitnej kategórie v zmysle článku 9 ods. 1 GDPR (t. j. údaje, „ktoré odhaľujú rasový alebo etnický pôvod“). Takéto údaje sú identifikované v GDPR, pretože si vyžadujú vyššiu mieru ochrany (Stanovisko 1/15 [2019] 3 C.M.L.R. 25 bod 141). Po druhé, základným návrhom zákona o ochrane údajov je, že predovšetkým právo na prístup dotknutej osoby má veľký význam ako brána k možnosti vykonávať ďalšie práva poskytované dotknutým osobám [pozri YS/Minister voor Immigratie, Integratie en Asiel (vec C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 bod 44].
59. Pán Knight identifikoval štyri body praktickej povahy. Po prvé, keď prevádzkovatelia nevysvetlia dotknutým osobám, že sa odvolávali na zákonnú výnimku, ani neposkytnú rozsiahle zhrnutie dôvodov, prečo tak konali, dotknutá osoba si nebude vedomá uplatnenia výnimky a v dôsledku toho ju nebude môcť účinne napadnúť. Po druhé, dotknuté osoby budú predovšetkým odkázané na to, aby prevádzkovatelia starostlivo uplatňovali výnimku opatrne a iba v nevyhnutných prípadoch. Hoci je ktorákoľvek dotknutá osoba oprávnená sťažovať sa komisárovi na uplatnenie výnimky alebo podať žalobu na súde, je pravdepodobné, že dotknutá osoba si nebude vedomá svojich práv a nebude mať za okolností, keď je potrebné pohotovo a presne dodržiavať práva na ochranu údajov, dostatok finančných prostriedkov na to, aby mohla podniknúť právne kroky. Po tretie, dotknutá osoba je ako prisťahovalec pravdepodobne v zraniteľnom postavení. Po štvrté, vo svetle dôkazov odporcov o použití imigračnej výnimky nejde o abstraktný problém (pozri vyššie bod 4).
60. Pán Knight naznačuje, že existuje úzka paralela medzi súčasnou výzvou voči imigračnej výnimke a odôvodnením súdu vo veci Christian Institute [2016] UKSC 51. Ako vo veci Christian Institute, tvrdí, že imigračná výnimka je široká, používa nevymedzené pojmy, uplatňuje nízku prahovú hodnotu, podlieha kontrolám, ktoré nie sú zjavné v samotnom ustanovení, a vzťahuje sa na veľmi širokú škálu kontextov a práv. Na rozdiel od veci Christian Institute neexistuje nijaké verejne dostupné usmernenie o imigračnej výnimke, nie to ešte so zákonným statusom, na ktorý sa musí brať ohľad.“

Európsku komisiu, aby poskytla ďalšie informácie o nevyhnutnosti a proporcionalite imigračnej výnimky, najmä so zreteľom na široký rozsah osobnej pôsobnosti.

75. **EDPB zároveň vyzýva Európsku komisiu, aby ďalej preskúmala, či v právnom rámci Spojeného kráľovstva existujú ďalšie záruky, alebo či by sa o nich mohlo uvažovať, napríklad prostredníctvom právne záväzných nástrojov, ktoré by dopĺňali imigračnú výnimku, čím by sa zvýšila jej predvídateľnosť a záruky pre dotknuté osoby, čím by sa takisto umožnilo lepšie a urýchlené posúdenie a monitorovanie požiadaviek nevyhnutnosti a proporcionality.**

3.1.2. Obmedzenia týkajúce sa následných prenosov

76. V článku 44 všeobecného nariadenia o ochrane údajov sa ustanovuje, že prenosy a následné prenosy osobných údajov sa uskutočňujú len vtedy, ak nebude ohrozená úroveň ochrany fyzických osôb zaručená všeobecným nariadením o ochrane údajov. Preto sa na osobné údaje prenášané z EHP do Spojeného kráľovstva na základe rozhodnutia o primeranosti vzťahuje v podstate rovnocenná úroveň ochrany, aká sa poskytuje podľa rámca EÚ na ochranu údajov. **To znamená, že nielen právne predpisy Spojeného kráľovstva budú „v podstate rovnocenné" s právnymi predpismi EÚ, pokiaľ ide o spracúvanie osobných údajov prenášaných do Spojeného kráľovstva na základe návrhu rozhodnutia, ale aj to, že pravidlami platnými v Spojenom kráľovstve týkajúcimi sa následného prenosu týchto údajov do tretích krajín sa zabezpečí, že sa bude naďalej poskytovať v podstate rovnocenná úroveň ochrany.**

77. V dôsledku toho je dôležité, aby bol každý následný prenos osobných údajov z EHP zo Spojeného kráľovstva do inej tretej krajiny riadne chránený zárukami alebo aby sa uskutočňoval v súlade s pravidlami o výnimkách[44], aby sa zabezpečila kontinuita ochrany poskytovanej právnymi predpismi EÚ. **Ak takúto ochranu nie je možné poskytnúť, následné prenosy osobných údajov EHP by sa nemali uskutočňovať.**

78. EDPB uznáva, že Spojené kráľovstvo vo veľkej miere zohľadnilo kapitolu V všeobecného nariadenia o ochrane údajov vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov (články 44 – 49) a v zákone o ochrane údajov z roku 2018[45]. **EDPB však určil určité aspekty legislatívneho rámca Spojeného kráľovstva, pokiaľ ide o následné prenosy, ktoré by mohli ohroziť úroveň ochrany osobných údajov prenášaných z EHP.**

79. **Prvá výzva**, ktorú EDPB určil, sa týka uznania tretích krajín, medzinárodných organizácií alebo území[46] Spojeným kráľovstvom ako primeraných príjemcov, podľa postupu vypracovaného v zákone o ochrane údajov z roku 2018. K následnému prenosu osobných údajov EHP zo Spojeného kráľovstva do iných tretích krajín môže naozaj dôjsť na základe budúceho možného nariadenia Spojeného kráľovstva o primeranosti[47].

80. Konkrétnejšie, ako je vysvetlené v odôvodnení 77 návrhu rozhodnutia, minister Spojeného kráľovstva má po konzultácii s ICO[48] právomoc uznať tretiu krajinu (alebo územie alebo sektor v rámci tretej krajiny), medzinárodnú organizáciu alebo opis takejto krajiny, územia, sektora alebo organizácie ako také, ktoré zabezpečujú primeranú úroveň ochrany osobných údajov. Pri posudzovaní primeranosti úrovne ochrany minister Spojeného kráľovstva musí vziať do úvahy rovnaké prvky, aké musí

[44] Pozri článok 49 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.
[45] Pozri § 17A, 17B, 17C a 18 zákona o ochrane údajov z roku 2018.
[46] Pozri § 17A zákona o ochrane údajov z roku 2018.
[47] Ekvivalent Spojeného kráľovstva s rozhodnutím o primeranosti podľa všeobecného nariadenia o ochrane údajov.
[48] Pozri § 182 ods. 2 zákona o ochrane údajov z roku 2018. Pozri aj memorandum o porozumení o úlohe Komisára pre informácie v súvislosti s novými posúdeniami primeranosti v Spojenom kráľovstve, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

posudzovať Európska komisia podľa článku 45 ods. 2 písm. a) až c) všeobecného nariadenia o ochrane údajov vykladaného spolu s odôvodnením 104 všeobecného nariadenia o ochrane údajov a ponechanou judikatúrou EÚ. To znamená, že pri posudzovaní primeranej úrovne ochrany poskytovanej treťou krajinou je relevantnou normou to, či daná tretia krajina zabezpečuje úroveň ochrany, ktorá je „v podstate rovnocenná" úrovni ochrany zaručenej v rámci Spojeného kráľovstva. Hoci EDPB berie na vedomie schopnosť Spojeného kráľovstva podľa všeobecného nariadenia Spojeného kráľovstva o ochrane údajov uznať územia za územia zabezpečujúce primeranú úroveň ochrany vzhľadom na rámec ochrany údajov Spojeného kráľovstva, EDPB chce zdôrazniť, že tieto uvedené územia nemusia mať dodnes prínos z rozhodnutia o primeranosti vydaným Európskou komisiou, ktorým sa zabezpečuje úroveň ochrany „v podstate rovnocenná" s úrovňou zaručenou v EÚ. To by mohlo viesť k možným rizikám pri ochrane poskytovanej osobným údajom prenášaným z EHP, najmä ak by sa rámec ochrany údajov Spojeného kráľovstva v budúcnosti odchýlil od *acquis* EÚ. Je potrebné poznamenať, že v júli 2020 viedol prelomový prípad Súdneho dvora EÚ Schrems II[49] k zrušeniu platnosti rozhodnutia Privacy Shield medzi EÚ a USA, keďže podľa Súdneho dvora EÚ sa právny rámec USA nemôže považovať za taký, ktorý poskytuje v podstate rovnocennú úroveň ochrany v porovnaní s úrovňou ochrany poskytovanou právnym rámcom EÚ. Prijaté rozsudky Súdneho dvora EÚ, ktoré sa v právnom rámci Spojeného kráľovstva považujú za ponechanú judikatúru, však už nemusia byť pre Spojené kráľovstvo záväzné, keďže Spojené kráľovstvo má po skončení preklenovacieho obdobia konkrétne možnosť zmeniť ponechané právne predpisy EÚ a jeho najvyšší súd nie je viazaný žiadnou ponechanou judikatúrou EÚ[50].

81. **EDPB vyzýva Európsku komisiu, aby pozorne sledovala postup a kritériá posudzovania primeranosti orgánmi Spojeného kráľovstva s ohľadom na iné tretie krajiny, najmä so zreteľom na tretie krajiny, ktoré EÚ neuznáva ako primerané podľa všeobecného nariadenia o ochrane údajov. Ak Európska komisia zistí, že tretia krajina, ktorú Spojené kráľovstvo považuje za primeranú, nezabezpečuje v podstate rovnocennú úroveň ochrany zaručenú v rámci EÚ, EDPB vyzýva Európsku komisiu, aby podnikla všetky potrebné kroky, ako je napríklad zmena rozhodnutia Spojeného kráľovstva o primeranosti v Spojenom kráľovstve s cieľom zaviesť osobitné záruky týkajúce sa osobných údajov pochádzajúcich z EHP a/alebo zvážiť pozastavenie rozhodnutia Spojeného kráľovstva o primeranosti v Spojenom kráľovstve, keď sú osobné údaje prenášané z EHP do Spojeného kráľovstva predmetom následných prenosov do príslušnej tretej krajiny na základe nariadenia Spojeného kráľovstva o primeranosti v Spojenom kráľovstve.**

82. **Druhá výzva** sa týka nadchádzajúceho preskúmania už existujúcich rozhodnutí o primeranosti vydaných Európskou komisiou podľa smernice 95/46/ES. Európska komisia môže po tomto preskúmaní rozhodnúť, že niektoré krajiny, ktoré mali až doteraz prínos z rozhodnutia o primeranosti, už neposkytujú v podstate rovnocennú úroveň ochrany s prihliadnutím na platné právne predpisy EÚ a nedávnu judikatúru. Ako je však uvedené v odseku 4 prílohy 21 k zákonu o ochrane údajov z roku 2018, Spojené kráľovstvo už uznalo tieto krajiny za krajiny poskytujúce primeranú úroveň ochrany. Aj keď minister Spojeného kráľovstva musí vykonať preskúmanie týchto záverov o primeranosti do štyroch rokov, Európska komisia vo svojom návrhu rozhodnutia poznamenáva, že tieto závery o primeranosti automaticky neprestanú existovať, ak minister Spojeného kráľovstva nevykoná požadované preskúmanie v stanovenej štvorročnej lehote[51].

[49] Pozri vec *Schrems II*.
[50] Pozri § 6 ods. 3 až 6 zákona o vystúpení z EÚ z roku 2018.
[51] Pozri odôvodnenie 82 návrhu rozhodnutia.

83. **EDPB vyzýva Európsku komisiu, aby sledovala, či po ukončení preskúmania už existujúcich rozhodnutí o primeranosti zo strany EÚ bude Spojené kráľovstvo krajinu považovanú za krajinu, ktorá už neposkytuje primeranú úroveň ochrany, stále považovať za takú. Ak je to tak, EDPB vyzýva Európsku komisiu, aby na základe odôvodnení 277 – 280 návrhu rozhodnutia prijala akékoľvek vhodné opatrenia na nápravu situácie, napríklad zmenou rozhodnutia o primeranosti s cieľom doplniť osobitné požiadavky na osobné údaje pochádzajúce z EHP a/alebo pozastavením rozhodnutia o primeranosti, ak sú osobné údaje prenášané z EHP do Spojeného kráľovstva predmetom následných prenosov do príslušnej tretej krajiny. EDPB vyzýva Európsku komisiu, aby pokračovala v tomto sledovaní počas obdobia trvania rozhodnutia Spojeného kráľovstva o primeranosti v Spojenom kráľovstve.**

84. **Tretia výzva** sa týka následného prenosu osobných údajov z EHP do krajín, ktoré nie sú vhodné, na základe nástrojov prenosu stanovených v článkoch 46 a 47 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. Hoci všeobecné nariadenie Spojeného kráľovstva o ochrane údajov poskytuje rovnaké nástroje prenosu ako tie, ktoré poskytuje všeobecné nariadenie o ochrane údajov, EDPB zdôrazňuje potrebu zabezpečiť, aby záruky, ktoré obsahujú, poskytovali účinnú ochranu v tretej krajine, najmä na základe rozsudku *Schrems II*.

85. Po rozhodnutí *Schrems II*, v ktorom Súdny dvor EÚ pripomína, že ochrana poskytovaná osobným údajom v EÚ musí sprevádzať údaje, nech smerujú kdekoľvek, EDPB už prijal počiatočné odporúčania týkajúce sa dodatočných opatrení[52] na pomoc vývozcom, ak je to potrebné, pri zabezpečovaní toho, aby sa dotknutým osobám poskytovala v podstate rovnocenná úroveň ochrany, aká je zaručená v rámci EÚ.

86. Podľa Súdneho dvora EÚ sú vývozcovia údajov zodpovední za overovanie, v závislosti od konkrétneho prípadu a, ak je to vhodné, v spolupráci s dovozcom údajov z tretej krajiny, či právne predpisy alebo prax tretej krajiny zasahujú do účinnosti príslušných záruk obsiahnutých v nástrojoch prenosu podľa článku 46 všeobecného nariadenia o ochrane údajov[53]. V takom prípade by vývozcovia údajov mali prijať dodatočné opatrenia, ktoré vyplnia tieto medzery v ochrane a zvýšia ju na úroveň požadovanú v právnych predpisoch EÚ.

87. **EDPB vyzýva Európsku komisiu, aby s cieľom zabezpečiť kontinuitu ochrany zaviedla do návrhu rozhodnutia ubezpečenia v tom zmysle, že keď vývozcovia údajov zo Spojeného kráľovstva použijú nástroje prenosu uvedené v článkoch 46 a 47 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov na následný prenos údajov prenášaných z EHP do iných tretích krajín, títo vývozcovia údajov posudzujú v závislosti od konkrétneho prípadu rámec ochrany údajov tretej krajiny a, ak je to potrebné, prijali vhodné opatrenia na zabezpečenie účinného dodržiavania záruk obsiahnutých vo zvolenom nástroji prenosu na zabezpečenie v podstate rovnocennej úrovne ochrany, aká je zaručená v rámci EÚ. EDPB zdôrazňuje, že bez týchto ubezpečení existuje riziko, že v podstate rovnocenná úroveň ochrany, ako je úroveň zaručená v EÚ, bude oslabená prostredníctvom následných prenosov, ktoré sa uskutočňujú zo Spojeného kráľovstva.**

88. **Štvrtá výzva** súvisiaca s následnými prenosmi sa týka medzinárodných dohôd, ktoré Spojené kráľovstvo uzatvorilo alebo ktoré má uzatvoriť v budúcnosti, a možného priameho prístupu orgánov z tretích krajín, ktoré sú zmluvnými stranami týchto dohôd, k osobným údajom z EHP. EDPB má skutočne silné obavy v súvislosti s už uzavretou dohodou medzi Spojeným kráľovstvom a USA o zákone CLOUD a Európska komisia uznáva túto výzvu so zdôraznením, že *„možné nadobudnutie*

[52] Pozri odporúčania EDPB 01/2020 o opatreniach, ktoré dopĺňajú nástroje na prenos s cieľom zabezpečiť súlad s úrovňou ochrany osobných údajov v EÚ, prijaté 10. novembra 2020, ktoré sa v súčasnosti dokončujú po verejnej konzultácii, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

[53] Pozri vec Schrems II, bod 134.

platnosti dohody môže mať vplyv na úroveň ochrany posudzovanú v tomto rozhodnutí“[54]. Na základe tejto dohody by sa po jej nadobudnutí platnosti osobné údaje prenášané z EHP do Spojeného kráľovstva podľa návrhu rozhodnutia potom skutočne mali riadiť ustanoveniami tejto dohody, v ktorej sa stanovujú podmienky priameho prístupu orgánov USA, čo by malo vplyv na rámec ochrany údajov Spojeného kráľovstva vrátane ustanovení o následných prenosoch. V dôsledku toho môžu mať na úroveň ochrany poskytovanú údajom prenášaným z EHP podstatný vplyv ustanovenia dohody uzatvorenej s USA a mať vplyv na úroveň ochrany týchto údajov. EDPB v tejto súvislosti poznamenáva, že Európska komisia odkazuje na vysvetlenia, ktoré poskytli orgány Spojeného kráľovstva v odôvodnení 153 jej návrhu rozhodnutia, bez uvedenia alebo poskytnutia konkrétneho písomného ubezpečenia alebo záväzku a takisto bez uvedenia konkrétnych právnych ustanovení podľa právnych predpisov Spojeného kráľovstva, ktoré by mali účinok na také vysvetlenia.

89. EDPB už predtým vyjadril tieto obavy v liste adresovanom Európskemu parlamentu z 15. júna 2020[55]. EDPB zdôraznil, že na základe „*acquis EÚ v oblasti ochrany údajov a najmä všeobecného nariadenia o ochrane údajov a smernice o presadzovaní práva*“, má EDPB výhrady k tomu, či by sa záruky v dohode o prístupe k osobným údajom v Spojenom kráľovstve uplatňovali za určitých okolností, pri ktorých by sa v prípade USA vyžadovali povinnosti týkajúce sa poskytovania údajov, ako aj toho, či sú tieto záruky dostatočné vzhľadom na normy EÚ, aby nedošlo k ohrozeniu úrovne ochrany poskytovanej v EÚ.

90. Ustanovenia dohody medzi Spojeným kráľovstvom a USA o zákone CLOUD môžu mať navyše významný vplyv na hmotnoprávne a procesné podmienky, za ktorých môžu mať americké orgány priamy prístup k osobným údajom uchovávaným prevádzkovateľmi alebo sprostredkovateľmi v Spojenom kráľovstve, čo má vplyv na úroveň ochrany zaručenú v rámci právnych predpisov Spojeného kráľovstva. Na zabezpečenie úrovne ochrany, ktorá je v podstate rovnocenná s úrovňou zaručenou podľa právnych predpisov EÚ, je napríklad „*nevyhnutné, aby záruky podľa takejto dohody obsahovali povinné predchádzajúce súdne povolenie ako základnú záruku prístupu k metaúdajom a obsahovým údajom*. *EDPB na základe svojho predbežného posúdenia, v ktorom zároveň konštatoval, že dohoda sa odvoláva na uplatňovanie vnútroštátneho práva, nemohol určiť také jasné ustanovenie v dohode uzavretej medzi Spojeným kráľovstvom a USA*“[56].

91. Zatiaľ čo Európska komisia zdôrazňuje, že údaje získané na základe tejto dohody by mali prínos z rovnocennej ochrany ako osobitné záruky poskytované takzvanou „zastrešujúcou dohodou medzi EÚ a USA“, EDPB má obavy, či by začlenenie týchto záruk do dohody medzi Spojeným kráľovstvom a USA o zákone CLOUD len na základe odkazu, ktorý sa uplatňuje *mutatis mutandis*, spĺňalo kritériá jasných, presných a prístupných pravidiel, pokiaľ ide o prístup k osobným údajom, alebo či by dostatočne zakotvilo tieto záruky, aby boli účinné a vykonateľné podľa právnych predpisov Spojeného kráľovstva.

92. **EDPB preto odporúča, aby Európska komisia objasnila, ako a na základe ktorého právneho nástroja by sa uviedli do platnosti rovnocenné ochrany ako osobitné záruky poskytované zastrešujúcou dohodou medzi EÚ a USA a mali by právne záväzný charakter podľa právnych predpisov Spojeného kráľovstva.**

93. EDPB takisto poznamenáva, že ustanovenia dohody medzi Spojeným kráľovstvom a USA o zákone CLOUD, vykladané v spojení s časťou 3 amerického zákona o CLOUD[57], vyvolávajú otázky týkajúce sa

[54] Pozri odôvodnenie 153 návrhu rozhodnutia.
[55] Pozri odpoveď EDPB europoslancom Sophie in’t Veld a Moritzovi Körner k dohode medzi USA a Spojeným kráľovstvom podľa amerického zákona CLOUD, prijatú 15. júna 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.
[56] Pozri vyššie uvedený list EDPB.
[57] Pozri americký zákon CLOUD, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

skutočného uplatňovania záruk, ktoré dohoda ponúka pre prístup orgánov presadzovania práva USA k osobným údajom v Spojenom kráľovstve spracúvaným poskytovateľmi elektronických komunikačných služieb alebo diaľkových počítačových služieb (ďalej len „poskytovatelia komunikačných služieb“), ktoré patria do jurisdikcie USA. Ak by poskytovateľ komunikačných služieb so sídlom v Spojenom kráľovstve podliehal právnym predpisom USA (napr. pretože je dcérskou spoločnosťou americkej spoločnosti), je potrebné určiť, či by americké orgány boli povinné v záujme získania týchto údajov opierať sa o dohodu medzi Spojeným kráľovstvom a USA o zákone CLOUD. Keďže Európska komisia zdôrazňuje, že *„osobitná pozornosť sa bude venovať uplatňovaniu a prispôsobovaniu ochrany zastrešujúcej dohody konkrétnemu typu prenosov, na ktoré sa vzťahuje dohoda medzi Spojeným kráľovstvom a USA“*, EDPB zdôrazňuje, že na základe predbežného posúdenia nie je jasné, či by sa záruky zakotvené v dohode medzi Spojeným kráľovstvom a USA o zákone CLOUD, a teda tá, ktorú poskytuje zastrešujúca dohoda medzi EÚ a USA, vzťahovali na všetky prípadné žiadosti o prístup k údajom v Spojenom kráľovstve, ktoré podali americké úrady podľa amerického zákona CLOUD.

94. V budúcnosti môže Spojené kráľovstvo uzavrieť ďalšie medzinárodné dohody alebo záväzky s tretími krajinami, ktoré by sa podľa návrhu rozhodnutia mohli vzťahovať na osobné údaje prenášané z EHP do Spojeného kráľovstva[58]. V závislosti od ustanovení týchto dohôd a uplatňovania osobitných ochranných doložiek môžu mať tieto medzinárodné dohody významný vplyv aj na hmotnoprávne a procesné podmienky prístupu orgánov tretích krajín k osobným údajom v Spojenom kráľovstve tým, že budú mať vplyv na rámec ochrany údajov Spojeného kráľovstva. Týka sa to najmä návrhu druhého dodatkového protokolu k Dohovoru Rady Európy o počítačovej kriminalite (ďalej len „Budapeštiansky dohovor“), o ktorom sa v súčasnosti rokuje medzi stranami tohto dohovoru, medzi ktoré patrí aj niekoľko krajín, ktoré nie sú členmi EÚ. Návrh protokolu skutočne obsahuje doložky, ktoré môžu strany svojvoľne aktivovať, napríklad pokiaľ ide o povolenie udeliť alebo neudeliť prístup k obsahovým údajom. Aj keď by všetky členské štáty EÚ aktivovali doložky v súlade s pravidlami EÚ o ochrane údajov, neposkytla sa žiadna záruka týkajúca sa Spojeného kráľovstva, ktoré by sa mohlo podstatne odchýliť od úrovne ochrany, ktorá by sa potom v tom čase poskytovala v rámci EÚ. Ďalším príkladom vyššie uvedených problémov je Dohoda medzi Spojeným kráľovstvom a Japonskom o komplexnom hospodárskom partnerstve[59] (ďalej len „CEPA“), čo je prvá obchodná dohoda Spojeného kráľovstva po brexite, ktorá vstúpila do platnosti 1. januára 2021[60] a ktorá obsahuje ustanovenia o osobných údajoch[61]. EDPB ďalej poznamenáva, že Spojené kráľovstvo takisto 1. februára 2021 formálne oznámilo svoju žiadosť o pripojenie sa ku komplexnému a progresívnemu Transpacifickému partnerstvu (ďalej len „CPTPP“), čo zahŕňa dohodu o Transpacifickom partnerstve (ďalej len „TPP“)[62].

95. EDPB poznamenáva, že okrem dohody medzi Spojeným kráľovstvom a USA o zákone CLOUD sa v návrhu rozhodnutia neriešia vyššie uvedené medzinárodné dohody.

[58] Pozri uvedený oddiel 2.3.3.

[59] Pozri Spojené kráľovstvo/Japonsko: Dohoda o komplexnom hospodárskom partnerstve [CS Japonsko č.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Pozri usmernenie vlády Spojeného kráľovstva k obchodným dohodám Spojeného kráľovstva s krajinami, ktoré nie sú členmi EÚ, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Podľa článku 8.80 ods. 5 CEPA sa strany zaväzujú, že podporia rozvoj mechanizmov na podporu zlučiteľnosti ich rôznych právnych prístupov k ochrane (osobných) údajov. Zmluvné strany sa podľa článku 8.84 zaväzujú, že nezakážu ani neobmedzia cezhraničný prenos informácií elektronickými prostriedkami vrátane osobných údajov, ak je táto činnosť zameraná na výkon podnikania osoby, na ktorú sa vzťahuje, v zmysle CEPA.

[62] Každá zmluvná strana umožní podľa článku 14.11 ods. 2 TPP cezhraničný prenos informácií elektronickými prostriedkami vrátane osobných údajov, ak je táto činnosť zameraná na výkon podnikania osoby, na ktorú sa vzťahuje.

96. **EDPB vyzýva Európsku komisiu, aby:**

- **Preskúmala vzájomný vzťah medzi rámcom ochrany údajov Spojeného kráľovstva a jeho medzinárodnými záväzkami, nad rámec dohody medzi Spojeným kráľovstvom a USA o zákone CLOUD, najmä s cieľom zabezpečiť kontinuitu úrovne ochrany v prípade následných prenosov osobných údajov prenášaných z EHP do Spojeného kráľovstva do iných tretích krajín na základe rozhodnutia o primeranosti v Spojenom kráľovstve a v prípade potreby nepretržite monitorovala a prijala opatrenia s ohľadom na uzatváranie ďalších medzinárodných dohôd medzi Spojeným kráľovstvom a tretími krajinami, ktoré by mohli ohroziť úroveň ochrany osobných údajov stanovenej v EÚ.**
- **Poskytla EDPB písomné záväzky orgánov Spojeného kráľovstva a určila konkrétne ustanovenia podľa právnych predpisov Spojeného kráľovstva v súvislosti s vysvetlením týkajúcim sa možného uplatňovania a vykonávania dohody medzi Spojeným kráľovstvom a USA o zákone CLOUD, ako sa uvádza v odôvodnení 153 návrhu rozhodnutia.**
- **V tejto súvislosti sledovala, či okrem záruk, ktoré by sa mohli poskytnúť primeraným vykonávaním prispôsobenia sa zastrešujúcej dohody medzi EÚ a USA, zabezpečuje dohoda medzi Spojeným kráľovstvom a USA o zákone CLOUD príslušné ďalšie záruky s cieľom zohľadniť úroveň citlivosti príslušných kategórií údajov a jedinečné požiadavky na prenos elektronických dôkazov priamo prostredníctvom poskytovateľov komunikačných služieb, a nie medzi orgánmi.**
- **Posúdila vplyv a potenciálne riziká ustanovení o osobných údajoch obsiahnutých v medzinárodných dohodách, ktoré nedávno podpísalo Spojené kráľovstvo, napríklad CEPA.**

97. **Piata** identifikovaná **výzva** sa týka uplatňovania výnimiek pre prenosy osobných údajov do tretej krajiny. Hoci sú dostupné výnimky podľa všeobecného nariadenia Spojeného kráľovstva o ochrane údajov rovnaké ako tie, ktoré sú ustanovené vo všeobecnom nariadení o ochrane údajov, je dôležité, aby ICO uplatňoval a pokračoval v uplatňovaní výkladu týkajúceho sa použitia týchto výnimiek v súlade s výkladom EDPB. V opačnom prípade, alebo ak sa Spojené kráľovstvo v budúcnosti odchýli od tohto výkladu, by hrozilo, že by sa mohla ohroziť úroveň ochrany údajov prenášaných z EHP do tretích krajín cez Spojené kráľovstvo.

98. **EDPB vyzýva Európsku komisiu, aby v rámci svojej monitorovacej úlohy osobitne skontrolovala, či je výklad Spojeného kráľovstva o používaní výnimiek v súlade s výkladom EÚ. Ak by však Spojené kráľovstvo postupovalo podľa odlišného výkladu používania výnimiek, čo by ohrozilo úroveň ochrany, je nevyhnutné, aby Európska komisia podnikla potrebné kroky tým, že zmení rozhodnutie o primeranosti, aby sa zabezpečilo, že úroveň ochrany poskytovaná osobným údajom EHP prenášaným do Spojeného kráľovstva nebude následne ohrozená, keď sa tieto údaje budú následne prenášať zo Spojeného kráľovstva do tretích krajín na základe iného výkladu výnimiek.**

99. **Šiesta výzva**, posledná v tomto oddiele, sa týka absencie ochrany poskytovanej podľa článku 48 všeobecného nariadenia o ochrane údajov v rámci ochrany údajov Spojeného kráľovstva.

100. Európska komisia vo svojom návrhu rozhodnutia skutočne objasňuje, že pri absencii nariadení o primeranosti alebo primeraných záruk môže dôjsť k prenosu iba na základe výnimiek stanovených v článku 49 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, *„s výnimkou článku 48 nariadenia (EÚ) 2016/679, ktoré sa Spojené kráľovstvo rozhodlo nezahrnúť do všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.“*[63] Absencia v podstate rovnocenného ustanovenia s článkom 48

[63] Pozri poznámka pod čiarou č. 78 návrhu rozhodnutia

všeobecného nariadenia o ochrane údajov zakotveného v rámci ochrany údajov Spojeného kráľovstva, pokiaľ ide o prenosy alebo poskytovanie údajov, na základe rozsudku súdneho orgánu alebo rozhodnutia správneho orgánu z inej tretej krajiny, môže viesť k právnej neistote v súvislosti s tým, či by bola podstatne ovplyvnená úroveň ochrany osobných údajov prenášaných z EHP do Spojeného kráľovstva podľa návrhu rozhodnutia.

101. EDPB vo svojom kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov zdôrazňuje, že pokiaľ ide o následné prenosy, *„ďalšie prenosy osobných údajov pôvodným príjemcom pôvodného prenosu údajov by sa mali povoliť len vtedy, keď ďalší príjemca takisto podlieha pravidlám poskytujúcim primeranú úroveň ochrany a dodržiava príslušné pokyny pri spracúvaní údajov v mene prevádzkovateľa.“*[64]. EDPB ďalej zdôrazňuje, že *„pôvodný príjemca údajov prenášaných z EÚ je povinný zabezpečiť, aby následné prenosy údajov poskytovali primerané záruky, ak neexistuje rozhodnutie o primeranosti. Takéto následné prenosy údajov by sa mali uskutočňovať len na obmedzené a určené účely a pokiaľ existuje právny základ na takéto spracúvanie“*[65]. Ako súčasť kapitoly V všeobecného nariadenia o ochrane údajov je pri posudzovaní toho, či právny rámec Spojeného kráľovstva v tomto ohľade zaručuje v podstate rovnocennú úroveň ochrany, potrebné v plnej miere zohľadniť článok 48[66].

102. EDPB v tejto súvislosti zdôrazňuje judikatúru Súdneho dvora EÚ vo vzťahu k riziku zneužitia alebo nezákonného prístupu a používania údajov, pričom osobitne uvádza, že *„pokiaľ ide o úroveň ochrany slobôd a základných práv zaručenú v rámci Únie, jej právna úprava obsahujúca zásah do základných práv zaručených článkami 7 a 8 Charty musí podľa ustálenej judikatúry Súdneho dvora stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie opatrenia a stanovujúce minimálne požiadavky spôsobom, aby osoby, ktorých osobné údaje boli dotknuté, mali dostatočné záruky, ktoré umožnia účinne chrániť ich údaje pred rizikami zneužitia, ako aj pred akýmkoľvek nezákonným prístupom a akýmkoľvek nezákonným použitím týchto údajov. Nevyhnutnosť disponovať takými zárukami je o to dôležitejšia v prípade, keď sú osobné údaje spracovávané automaticky a keď existuje značné riziko nezákonného prístupu k týmto údajom“*[67].

103. EDPB v tejto súvislosti poznamenáva, že na základe informácií, ktoré sú k dispozícii v návrhu rozhodnutia, sa v rámci ochrany údajov Spojeného kráľovstva jasne nestanovuje, že akýkoľvek rozsudok súdneho orgánu a akékoľvek rozhodnutie správneho orgánu tretej krajiny, ktoré si na prenos alebo poskytnutie osobných údajov vyžaduje prevádzkovateľa alebo sprostredkovateľa, možno uznať alebo vykonať akýmkoľvek spôsobom iba na základe medzinárodnej dohody platnej medzi žiadajúcou treťou krajinou a Spojeným kráľovstvom. Článok 48 všeobecného nariadenia o ochrane údajov je základným ustanovením podľa kapitoly V všeobecného nariadenia o ochrane údajov, pretože sa v ňom vyžaduje, že prenos alebo poskytnutie osobných údajov na základe rozsudku alebo rozhodnutia súdneho orgánu alebo správneho orgánu v tretej krajine sa môže uznať alebo vykonať iba na základe platnej medzinárodnej dohody medzi žiadajúcou treťou krajinou a Úniou alebo členským štátom bez toho, aby boli dotknuté iné dôvody prenosu podľa kapitoly V všeobecného nariadenia o ochrane údajov. EDPB skutočne pripomína, že *„žiadosť zahraničného orgánu sama osebe nepredstavuje právny dôvod prenosu. Príkaz je možné uznať iba, ak sa zakladá na medzinárodnej dohode, ako je napríklad zmluva o vzájomnej právnej pomoci, platnej medzi*

[64] Pozri WP254 rev.01, s. 6.
[65] Pozri WP254 rev.01, s. 6.
[66] Pozri článok 44 všeobecného nariadenia o ochrane údajov, posledná veta, najmä: *„Všetky ustanovenia v tejto kapitole sa uplatňujú s cieľom zabezpečiť, aby sa neohrozila úroveň ochrany fyzických osôb zaručená týmto nariadením.“*
[67] Pozri vec Schrems I, bod 91.

žiadajúcou treťou krajinou a Úniou alebo členským štátom'"[68]. Je preto nevyhnutné, aby podľa právnych predpisov Spojeného kráľovstva bolo možné určiť v podstate rovnocenné ustanovenia.

104. Európska komisia v návrhu rozhodnutia uvádza vysvetlenia zo strany orgánov Spojeného kráľovstva, podľa ktorých ani common law, ani právne predpisy neumožňujú vykonanie zahraničného rozsudku v Spojenom kráľovstve, v ktorom sa požadujú údaje, bez medzinárodnej dohody a každý prenos údajov na základe žiadosti zahraničného súdu alebo správneho orgánu si vyžaduje nástroj, akým je napríklad právny predpis o primeranosti alebo primeraná záruka, pokiaľ sa neuplatňuje výnimka podľa článku 49 nariadenia Spojeného kráľovstva o ochrane údajov. V tejto súvislosti však EDPB neboli poskytnuté informácie o výmenách medzi Európskou komisiou a orgánmi Spojeného kráľovstva[69], a preto nie je schopný analyzovať a nezávisle posúdiť, či sú záruky poskytnuté orgánmi Spojeného kráľovstva dostatočné na to, aby sa zabezpečila v podstate rovnocenná úroveň ochrany v súvislosti so zárukami stanovenými v článku 48 všeobecného nariadenia o ochrane údajov.

105. **EDPB vyzýva Európsku komisiu, aby poskytla ďalšie uistenia a konkrétne odkazy na právne predpisy Spojeného kráľovstva, ktorými sa zabezpečuje úroveň ochrany podľa právneho rámca Spojeného kráľovstva, ktorá v podstate zodpovedá úrovni zaručenej na území EHP. EDPB preto vyzýva Európsku komisiu, aby poskytla písomné vysvetlenia a záväzky od orgánov Spojeného kráľovstva súvisiace s vykonávaním ochrany, ktorá v podstate zodpovedá ochrane stanovenej v článku 48 všeobecného nariadenia o ochrane údajov.**

106. **EDPB sa domnieva, že identifikácia ustanovení v rámci právnych predpisov Spojeného kráľovstva, ktorými sa zabezpečuje v podstate rovnocenná úroveň ochrany v súvislosti so zárukami stanovenými v článku 48 všeobecného nariadenia o ochrane údajov, je o to dôležitejšia so zreteľom na už vznesené obavy týkajúce sa žiadostí zo strany USA alebo orgánov iných tretích krajín o prístup k údajom v Spojenom kráľovstve, ako aj so zreteľom na to, že podľa rozhodnutia o primeranosti by sa mohli osobné údaje prenášať z EHP do Spojeného kráľovstva bez ďalších záruk alebo právnych záväzkov príjemcu vzťahujúcich sa na žiadosti o prístup k údajom zo strany orgánov ďalších tretích krajín.**

3.2. Procesné mechanizmy a mechanizmy presadzovania

107. EDPB na základe kritérií stanovených v kritériu primeranosti podľa všeobecného nariadenia o ochrane údajov zanalyzoval tieto v návrhu uvedené aspekty rámca ochrany údajov Spojeného kráľovstva: existencia a účinné pôsobenie nezávislého dozorného orgánu, existencia systému zabezpečujúceho dobrú úroveň súladu, a systém na prístup k primeraným mechanizmom nápravy, ktorý jednotlivcom v EÚ poskytuje prostriedky na uplatňovanie svojich práv a vymáhanie nápravy bez komplikovaných prekážok v správnych a súdnych prostriedkoch nápravy.

3.2.1. Príslušný nezávislý dozorný orgán

108. EDPB víta úsilie Európskej komisie o komplexné preskúmanie zriadenia, fungovania a právomocí dozorného orgánu Spojeného kráľovstva uvedeného v kapitole 2.6. návrhu rozhodnutia. Úlohou Komisára pre informácie (ďalej len „IC“) [Information Commissioner] v spojenom kráľovstve je dohľad a presadzovanie súladu s nariadením Spojeného kráľovstva o ochrane údajov a zákonom o ochrane údajov z roku 2018.

[68] Pozri prílohu k spoločnej reakcii EDPB a EDPS k výboru LIBE o vplyve amerického zákona o objasnení zákonného využívania údajov v zámorí na európsky právny rámec na ochranu osobných údajov, ktorý bol prijatý 10. júla 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[69] Pozri poznámka pod čiarou č. 78 návrhu rozhodnutia

Podľa prílohy 12 k zákonu o ochrane osobných údajov z roku 2018 je IC „Corporation Sole“, t. j. samostatný právny subjekt zložený z jednej osoby, ktorý podporuje Úrad komisára pre informácie (ďalej len „ICO“).

109. Pokiaľ ide o nezávislosť IC, EDPB zdôrazňuje, že článok 51 nariadenia Spojeného kráľovstva o ochrane údajov neobsahuje výslovné objasnenie, že IC je nezávislý orgán verejnej moci, ako sa to uvádza v článku 51 všeobecného nariadenia o ochrane údajov v súvislosti s dozornými orgánmi. EDPB však uznáva, že nariadenie Spojeného kráľovstva o ochrane údajov podobne odzrkadľuje vo svojom článku 52 príslušné pravidlá týkajúce sa nezávislosti, ktoré sú stanovené v článku 52 ods. 1 až 3 všeobecného nariadenia o ochrane údajov.

110. EDPB okrem toho podotýka, že článok 52 nariadenia Spojeného kráľovstva o ochrane údajov neobsahuje povinnosti, ktoré zodpovedajú článku 52 ods. 4 až 6 všeobecného nariadenia o ochrane údajov, v ktorom sa výslovne zabezpečuje, že príslušnému dozornému orgánu sa poskytujú zdroje potrebné na účinné plnenie jeho úloh a vykonávanie jeho právomocí. EDPB však uznáva, že zákon o ochrane údajov z roku 2018 obsahuje ustanovenia, ktorých cieľom je zabezpečiť primerané financovanie ICO[70], ako aj okolnosť, že ICO je v súčasnosti jedným z najväčších dozorných orgánov v porovnaní s dozornými orgánmi v rámci EÚ/EHP. Keďže nepretržité prideľovanie primeraných zdrojov, najmä pokiaľ ide o zamestnancov a rozpočet[71], je nevyhnutné na zabezpečenie riadneho fungovania dozorného orgánu na plnenie všetkých pridelených úloh a Európsky parlament ho nedávno označil ako dôležité[72], EDPB považuje za nevyhnutné venovať osobitnú pozornosť budúcemu vývoju v tejto oblasti.

111. **EDPB preto vyzýva Európsku komisiu, aby pozorovala vývoj v súvislosti s prideľovaním zdrojov ICO, ktorý by mal nepriaznivý vplyv na riadne plnenie jeho úloh.**

3.2.2. Existencia systému ochrany údajov zabezpečujúceho dobrú úroveň súladu

112. S cieľom zabezpečiť monitorovanie a presadzovanie právnych predpisov sa v návrhu rozhodnutia vykonáva komplexné preskúmanie právomocí ICO podľa článku 58 nariadenia Spojeného kráľovstva o ochrane údajov a zákona o ochrane údajov z roku 2018. EDPB uznáva, že článok 58 nariadenia Spojeného kráľovstva o ochrane údajov podrobne odzrkadľuje príslušné pravidlá týkajúce sa právomocí dozorných orgánov, ktoré sú stanovené v článku 58 všeobecného nariadenia o ochrane údajov. Pokiaľ ide o právomoc ukladať správne pokuty v závislosti od okolností každého jednotlivého prípadu, článok 83 nariadenia Spojeného kráľovstva o ochrane údajov obsahuje ustanovenia a maximálne sumy podobné ustanoveniam v článku 83 všeobecného nariadenia o ochrane údajov. EDPB sa preto domnieva, že súčasný právny rámec Spojeného kráľovstva v tejto oblasti je v súlade s normami stanovenými v príslušných právnych predpisoch EÚ. EDPB však v tejto súvislosti zdôrazňuje, že existencia *účinných* sankcií zohráva dôležitú úlohu pri zabezpečovaní dodržiavania pravidiel.[73]

113. **Vzhľadom na uvedené skutočnosti EDPB vyzýva Európsku komisiu, aby monitorovala účinnosť sankcií a príslušných prostriedkov nápravy rámca ochrany údajov Spojeného kráľovstva.**

[70] Pozri § 137, 138, 182 a prílohu 12 ods. 9 k zákonu o ochrane údajov z roku 2018.
[71] Pozri WP 254 rev.01, s. 7.
[72] Uznesenie Európskeho parlamentu z 25. marca 2021 o hodnotiacej správe Komisie o vykonávaní všeobecného nariadenia o ochrane údajov dva roky od jeho uplatňovania, bod 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.html.
[73] Pozri WP 254 rev.01, s. 7.

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

114. Základnými prvkami posudzovania, či systém ochrany údajov poskytuje primeranú úroveň ochrany, sú účinný mechanizmus dohľadu, ktorý umožňuje nezávislé prešetrovanie sťažností, aby sa identifikovali a potrestali porušenia práv dotknutej osoby v praxi, ako aj účinné správne a súdne prostriedky nápravy (vrátane náhrady škôd v dôsledku nezákonného spracúvania osobných údajov dotknutej osoby).

115. EDPB víta, že ICO poskytuje na svojom webovom sídle komplexné informácie a usmernenia, ktorých cieľom je zvýšiť informovanosť prevádzkovateľov a sprostredkovateľov údajov v súvislosti s ich záväzkami a povinnosťami, ako aj podporovať dotknuté osoby, aby boli oboznámení o svojich právach týkajúcich sa ich osobných údajov a aby presadzovali svoje individuálne práva podľa nariadenia Spojeného kráľovstva o ochrane údajov a zákona o ochrane údajov z roku 2018.

116. **Bez ohľadu na súčasný stav EDPB vyzýva Európsku komisiu, aby nepretržite pozorovala úroveň podpory, ktorú ICO poskytuje predovšetkým jednotlivcom, ktorých osobné údaje sa preniesli do Spojeného kráľovstva na základe rozhodnutia o primeranosti, na účely pomoci pri uplatňovaní ich práv v rámci režimu ochrany údajov v Spojenom kráľovstve.**

4. PRÍSTUP K OSOBNÝM ÚDAJOM PRENÁŠANÝM Z EÚ ORGÁNMI VEREJNEJ MOCI V SPOJENOM KRÁĽOVSTVE A ICH POUŽÍVANIE TÝMITO ORGÁNMI

4.1. Prístup a používanie zo strany orgánov verejnej moci Spojeného kráľovstva na účely presadzovania práva v trestných veciach

4.1.1. Právne základy a uplatniteľné obmedzenia/záruky

117. Pokiaľ ide o posúdenie, ktoré vykonala Európska komisia a ktoré bolo uvedené v odôvodneniach 132 a ďalej návrhu rozhodnutia o **prístupe na účely presadzovanie práva**, Európska komisia poskytuje diferencované a podrobné informácie a vo všeobecnosti dospieva k zrozumiteľným záverom. EDPB preto upúšťa od opakovania väčšiny faktických zistení a posúdení v tomto stanovisku. Existujú však určité prípady, pri ktorých opis skutočností alebo vysvetlenie záverov nepostačuje na to, aby sa s nimi EDPB mohol stotožniť.

4.1.1.1. Využitie súhlasu

118. EDPB berie na vedomie, že Európska komisia v poznámke č. 184 návrhu rozhodnutia uvádza[74], že **využitie súhlasu** nie je relevantné v prípade scenára primeranosti, keďže v prípade prenosu údaje od dotknutej osoby nezhromažďuje priamo orgán presadzovania práva Spojeného kráľovstva na základe súhlasu. Využitie súhlasu ako právny základ policajnej činnosti preto neposudzuje Európska komisia.

119. EDPB v tejto súvislosti pripomína, že v článku 45 ods. 2 písm. a) všeobecného nariadenia o ochrane údajov sa vyžaduje posúdenie širokej škály prvkov, ktoré sa neobmedzujú len na situáciu prenosu a medzi ktoré patrí *„právny štát, dodržiavanie ľudských práv a základných slobôd, príslušné právne predpisy, a to všeobecné aj odvetvové, vrátane [...] trestného práva“*.

120. Na základe informácií poskytnutých Európskou komisiou v odôvodnení 38 jej návrhu vykonávacieho rozhodnutia v zmysle smernice Európskeho parlamentu a Rady (EÚ) 2016/680 o primeranej ochrane osobných údajov Spojeným kráľovstvom (ďalej len „návrh rozhodnutia o primeranosti smernice

[74] Pozri s. 37 návrhu rozhodnutia.

o presadzovaní práva“) EDPB takisto berie na vedomie, že využitie súhlasu by si podľa vymedzenia v režime Spojeného kráľovstva v kontexte presadzovania práva vždy vyžadovalo uplatniteľný právny základ. To znamená, že aj keď polícia má zákonné právomoci na spracúvanie údajov na účely vyšetrovania, za určitých konkrétnych okolností (napríklad na získanie vzorky DNA) môže polícia považovať za vhodné požiadať dotknutú osobu o súhlas.

121. **EDPB vyzýva Európsku komisiu, aby do rozhodnutia o primeranosti zapracovala analýzu o možnom využití súhlasu v kontexte presadzovania práva, ktorá sa uvádza v návrhu rozhodnutia o primeranosti smernice o presadzovaní práva.**

4.1.1.2. Príkazy na domovú prehliadku a príkazy na predloženie dôkazov

122. Napriek tomu, že EDPB vo všeobecnosti nemá pripomienky k získavaniu dôkazov políciou prostredníctvom príkazov na domovú prehliadku a príkazov na predloženie dôkazov, z odôvodnenia 136 návrhu rozhodnutia vyplýva, že Európska komisia sústredila svoje úvahy o prístupe k presadzovaniu práva okolo polície a že spracúvanie osobných údajov inými orgánmi presadzovania práva bolo preskúmané v menšej miere.

123. Napríklad vo Vysvetľujúcom rámci Spojeného kráľovstva pre diskusiu o primeranosti, oddiele F s názvom „Presadzovanie práva“[75] sa na s. 11 tvrdí, že **Národná kriminálna agentúra,** ktorá okrem iného disponuje širšou funkciou pre kriminálne spravodajské informácie, by mohla predstavovať orgán presadzovania práva osobitného záujmu. Národná kriminálna agentúra opisuje svoju úlohu ako spájanie spravodajských informácií z rôznych zdrojov s cieľom maximalizovať príležitosti na analýzu, posúdenie a taktickú prácu, a to vrátane spravodajských informácií z technického zachytávania komunikácie a spolupráce s partnermi v oblasti presadzovania práva v Spojenom kráľovstve a v zahraničí, bezpečnostnými a spravodajskými agentúrami[76]. Národná kriminálna agentúra je takisto jedným z hlavných účastníkov medzinárodného partnerstva pre presadzovanie práva a zohráva kľúčovú úlohu pri výmene kriminálneho spravodajstva[77].

124. EDPB okrem toho upozorňuje, že Vládne komunikačné ústredie, ktorého činnosť bežne patrí do rozsahu pôsobnosti časti 4 zákona o ochrane údajov z roku 2018, t. j. národná bezpečnosť, je takisto

[75] Pozri Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel F s názvom „Presadzovanie práva“, 13. marca 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Pozri webovú lokalitu Národnej kriminálnej agentúry, *Intelligence: enhancing the picture of serious organised crime affecting the UK* (Spravodajské informácie: lepšie vykreslenie obrazu závažnej organizovanej trestnej činnosti zasahujúcej Spojené kráľovstvo), https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Hoci nie všetky spravodajské informácie, ktoré spracúva Národná kriminálna agentúra, prestavujú osobné údaje, takéto údaje môžu tvoriť ich významnú časť a činnosti, ktoré sú tu opísané, sa líšia od klasickej policajnej práce. Preto by posúdenie prístupu k osobným údajom zo strany orgánov presadzovania práva v Spojenom kráľovstve bolo bez podrobného posúdenia činností Národnej kriminálnej agentúry neúplné. Zdá sa rozumné uistiť sa, že zásady ochrany údajov majú rovnaký význam vo všetkých relevantných agentúrach presadzovania práva, a teda pozrieť sa podrobnejšie na agentúru ako Národná kriminálna agentúra, ktorej práca je obzvlášť založená na údajoch. Navyše v časti *Looking to the future* (Pohľad do budúcnosti) sa ďalej vysvetľuje: *„Neustále vyhľadávame nové príležitosti na získavanie, rozvoj a vylepšovanie tradičných možností zvyšovania kvantity a kvality spravodajských informácií, ktoré sú k dispozícii na využitie v Spojenom kráľovstve aj v zahraničí.“ „V rámci toho, s využitím právomocí zverených agentúre zákonom o trestnej činnosti a súdoch, vyvíjame nový nástroj National Data Exploitation Capability s cieľom získať prístup k údajom, ktorými disponuje verejná správa, prepojiť ich a využívať.“* […] *„Všetky tieto aktivity zvýšia našu akcieschopnosť a flexibilitu, aby sme mohli reagovať na nové hrozby a pôsobiť proaktívne, zhromažďovať a analyzovať informácie a spravodajské informácie o vznikajúcich hrozbách, a tak prijať opatrenia predtým, ako sa tieto hrozby uskutočnia.“*

aktívne pri redukovaní spoločenských a finančných škôd, ktoré závažná a organizovaná trestná činnosť spôsobuje Spojenému kráľovstvu, pričom úzko spolupracuje s ministerstvom vnútra, Národnou kriminálnou agentúrou, daňovými a colnými orgánmi jej veličenstva a ostatnými ministerstvami[78]. Jeho činnosti sa týkajú boja proti pohlavnému zneužívaniu detí, podvodu, ďalších druhov hospodárskej trestnej činnosti vrátane prania špinavých peňazí, zločinného využívania technológií, boja proti počítačovej kriminalite, organizovanej trestnej činnosti vrátane obchodovania s ľuďmi, a drog, strelných zbraní a iných nezákonných aktivít pašovania.

125. **EDPB vyzýva Európsku komisiu, aby doplnila svoju analýzu o analýzu agentúr, ktoré aktívne pôsobia v oblasti presadzovania práva a ktoré sa vo svojej každodennej činnosti zrejme zameriavajú na získavanie a analýzu údajov vrátane osobných údajov, najmä Národnej kriminálnej agentúry. Okrem toho vyzýva Komisiu, aby podrobnejšie preskúmala agentúry ako Vládne komunikačné ústredie, ktorých činnosti patria do rozsahu pôsobnosti presadzovania práva aj národnej bezpečnosti, ako aj právny rámec, ktorý sa na ne vzťahuje pri spracúvaní osobných údajov.**

4.1.1.3. Vyšetrovacie právomoci na účely presadzovania práva

126. V rámci kapitoly 4 referenčného kritéria primeranosti podľa všeobecného nariadenia o ochrane údajov s názvom „Základné záruky pre **presadzovanie práva v tretích krajinách** a prístup národnej bezpečnosti k obmedzeným zásahom do základných práv“ EDPB pripomína, že *„[v] tejto súvislosti súd takisto kriticky poznamenal, že predchádzajúce rozhodnutie o Safe Harbor, neobsahovalo žiadne zistenia týkajúce sa existencie pravidiel prijatých štátom v Spojených štátoch s cieľom obmedziť akýkoľvek zásah do základných práv osôb, ktorých údaje sú prenášané z Európskej únie do Spojených štátov – **zásah, ktorý by boli štátne subjekty tejto krajiny poverené využiť pri dosahovaní legitímnych cieľov**, ako je národná bezpečnosť.“*[79] V tomto referenčnom kritériu EDPB uvádza, že **štyri európske základné záruky**[80] **sa musia rešpektovať na to, aby sa prístup k údajom** všetkými tretími krajinami, či už na účely národnej bezpečnosti alebo **na účely presadzovania práva, mohol považovať za primeraný**, predovšetkým sa **musí preukázať nevyhnutnosť a proporcionalita týkajúca sa sledovaných legitímnych cieľov.**

127. Európska komisia v tomto oddiele návrhu rozhodnutia dospieva k záveru (odôvodnenie 139), že *„keďže tieto vyšetrovacie právomoci, ktoré stanovuje zákon o vyšetrovacích právomociach z roku 2016, sú rovnaké ako tie, ktoré majú k dispozícii národné bezpečnostné služby, podmienky, obmedzenia a záruky uplatniteľné na takéto právomoci sú podrobnejšie rozobraté v oddiele o prístupe k osobným údajom a ich používaní zo strany orgánov verejnej moci Spojeného kráľovstva na účely národnej bezpečnosti.“* Z judikatúry Súdneho dvora EÚ však vyplýva, že legitímne ciele, ako je národná bezpečnosť alebo boj proti závažným trestným činom, sa pri overovaní kritéria nevyhnutnosti a proporcionality právnych predpisov členských štátov umožňujúcich uchovávanie osobných údajov orgánmi verejnej moci a prístup k nim líšia, pričom by bolo možné odôvodniť určitý druh zásahu, iné však nie[81].

128. **EDPB by preto v rámci rozhodnutia uvítal konkrétne posúdenie nevyhnutnosti a proporcionality podmienok, obmedzení a záruk uvedených v odôvodneniach 174 a ďalej – ide o oddiel vyhradený pre opatrenia na dosahovanie cieľov v záujme národnej bezpečnosti – pokiaľ ide o uplatňovanie týchto podmienok, obmedzení a záruk v kontexte opatrení na dosahovanie cieľov presadzovania práva. Európsku komisiu preto vyzýva, aby ďalej objasnila, či sú uvedené uchovávanie osobných**

[78] Pozri webovú lokalitu Vládneho komunikačného ústredia, časť *Mission* (Poslanie), *Serious and Organised Crime* (Závažná a organizovaná trestná činnosť), https://www.gchq.gov.uk/section/mission/serious-crime.
[79] Pozri WP254 rev.01, s. 9.
[80] Pozri odporúčania EDPB 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania.
[81] Pozri Súdny dvor EÚ, spojené veci C-511/18, C-512/18 a C-520/18, La Quadrature du Net a ďalší, 6. október 2020, ECLI:EU:C:2020:791.

údajov a prístup k nim na účely presadzovania práva dostatočne obmedzené na zabezpečenie v podstate rovnocennej úrovne ochrany, aká je zaručená v rámci EÚ.

4.2.1. Ďalšie používanie získaných informácií na účely presadzovania práva (odôvodnenie 140 až 154)

129. EDPB berie na vedomie, že rámec ochrany údajov Spojeného kráľovstva poskytuje podobné záruky a obmedzenia, ako sú tie, ktoré sa poskytujú v rámci právnych predpisov EÚ v súvislosti s ďalším používaním získaných informácií na účely presadzovania práva.

4.1.2.1. Ďalšie používanie na ďalšie účely presadzovania práva

130. V zákone o ochrane údajov z roku 2018 sa stanovuje, že osobné údaje získané príslušným orgánom na účely presadzovania práva sa môžu ďalej spracúvať (či už pôvodným prevádzkovateľom alebo iným prevádzkovateľom) na akýkoľvek iný účel presadzovania práva za predpokladu, ak je prevádzkovateľ zo zákona oprávnený spracúvať údaje na tento iný účel a predmetné spracúvanie je na daný účel nevyhnutné a primerané. Európska komisia berie do úvahy, že sa na spracúvanie vykonávané prijímajúcim orgánom uplatnia všetky záruky stanovené v časti 3 zákona o ochrane údajov z roku 2018. EDPB však zdôrazňuje, že v § 44 ods. 4, 45 ods. 4, 48 ods. 3 a 68 ods. 7 časti 3 zákona o ochrane údajov z roku 2018 sa stanovuje možnosť obmedziť práva dotknutej osoby, pričom v § 79 sa stanovuje možnosť vydať osvedčenie, ktorým sa dokazuje, že obmedzenie je nevyhnutným a proporcionálnym opatrením v záujme ochrany národnej bezpečnosti. **EDPB preto odporúča, aby Európska komisia ďalej posúdila možný vplyv takýchto obmedzení na úroveň ochrany osobných údajov v súvislosti s ďalším používaním získaných informácií. Podobne by sa malo poskytnúť ďalšie objasnenie v súvislosti právnym rámcom Spojeného kráľovstva, ktoré umožňuje takéto následné poskytovanie údajov, najmä zákon o digitálnom hospodárstve z roku 2017, ako aj zákon o trestnej činnosti a súdoch z roku 2013, ktorým sa umožňuje poskytovanie údajov Národnej kriminálnej agentúre.**

4.1.2.2. Ďalšie používanie na účely iné ako presadzovanie práva v Spojenom kráľovstve

131. V zákone o ochrane údajov z roku 2018 sa zároveň stanovuje, že osobné údaje získané na akýkoľvek účel presadzovania práva sa môžu spracúvať na účel, ktorý nie je presadzovaním práva, ak je spracúvanie povolené zákonom. Právny základ, ktorým sa v tomto prípade oprávňuje takéto poskytovanie údajov, je § 19 zákona o boji proti terorizmu z roku 2008. EDPB v tejto súvislosti poznamenáva, že rozsah pôsobnosti a ustanovenia § 19 zákona o boji proti terorizmu nie sú v uspokojivej miere predmetom posúdenia Európskej komisie a môžu znamenať ďalšie používanie širšej povahy, najmä pokiaľ ide o § 19 ods. 2, v ktorom sa stanovuje, že *„[i]nformácie získané ktoroukoľvek zo spravodajských služieb pri výkone ktorejkoľvek zo svojich funkcií sa môžu použiť danou službou v súvislosti s výkonom ktorejkoľvek zo svojich iných funkcií.“*

132. EDPB zároveň poznamenáva, že odkaz Európskej komisie na skutočnosť, že príslušné orgány sú orgánmi verejnej moci, ktoré musia konať v súlade s EDĽP vrátane jeho článku 8, čím sa zabezpečuje, že každé poskytnutie údajov medzi orgánmi presadzovania práva a spravodajskými službami je v súlade s právnymi predpismi o ochrane údajov a EDĽP, by sa mohol ďalej podložiť identifikovaním príslušných zákonov a právnych predpisov v rámci právneho poriadku Spojeného kráľovstva, ktorými sa jasne a presne stanovujú takéto obmedzenia.

4.1.2.3. Ďalšie používanie v kontexte následných prenosov mimo Spojeného kráľovstva

133. Hoci Európska komisia poukazuje na skutočnosť, že dohoda medzi Spojeným kráľovstvom a USA na základe zákona o objasnení zákonného využívania údajov v zámorí (dohoda medzi Spojeným kráľovstvom a USA o zákone CLOUD) môže mať vplyv na následné prenosy od poskytovateľov komunikačných služieb v Spojenom kráľovstve do Spojených štátov, EDPB takisto zdôrazňuje, že vstup tejto dohody do platnosti

môže mať vplyv aj na ďalšie používanie získaných informácií prostredníctvom následných prenosov od orgánov presadzovania práva v Spojenom kráľovstve, najmä vo vzťahu k vydávaniu a prenosu príkazov podľa článku 5 dohody medzi Spojeným kráľovstvom a USA o zákone CLOUD.

134. EDPB sa v širšom zmysle domnieva, že uzatvorenie budúcich dvojstranných dohôd s tretími krajinami na účely spolupráce pri presadzovaní práva, čím sa poskytne právny základ na prenos osobných údajov do týchto krajín, môže takisto zásadne vplývať na podmienky ďalšieho používania získaných informácií, keďže takéto dohody môžu mať vplyv na posudzovaný rámec ochrany údajov Spojeného kráľovstva. EDPB preto Európskej komisii odporúča, aby ďalej posúdila tento bod, identifikujúc existenciu medzinárodných dohôd, a objasnila, či ustanovenia v týchto dohodách môžu vplývať na uplatňovanie právnych predpisov Spojeného kráľovstva o ochrane údajov a poskytla ďalšie obmedzenia alebo výnimky týkajúce sa ďalšieho používania získaných informácií na účely presadzovania práva a ich poskytovania do zahraničia. EDPB sa domnieva, že tieto informácie a posúdenie sú kľúčové na umožnenie komplexného posúdenia úrovne ochrany poskytovanej právnym rámcom Spojeného kráľovstva a praktikami v súvislosti s poskytovaním údajov do zahraničia a ich ďalším používaním.

4.3.1. Dohľad

135. EDPB poznamenáva, že dohľad nad agentúrami presadzovania trestného práva zabezpečuje okrem ICO aj kombinácia rôznych komisárov. V návrhu zistení primeranosti sa uvádza Komisár pre vyšetrovacie právomoci (IPC), Komisár pre uchovávanie a používanie biometrického materiálu [the Commissioner for the Retention and Use of Biometric Material], ako aj Komisár pre sledovanie kamerovým systémom [the Surveillance Camera Commissioner]. V tejto súvislosti treba poznamenať, že Súdny dvor EÚ opakovane zdôrazňuje potrebu nezávislého dohľadu. Komisár pre vyšetrovacie právomoci má osobitný význam, pokiaľ ide o otázky prístupu k osobným údajom preneseným do Spojeného kráľovstva. EDPB to chápe tak, že Komisár pre vyšetrovacie právomoci je tzv. Komisár pre justíciu, podobne ako iní Komisári pre justíciu, ktorí sa uvádzajú v súvislosti s kapitolou o národnej bezpečnosti, a že títo Komisári pre justíciu majú nezávislosť ako sudcovia aj pri výkone funkcie komisárov. Pokiaľ ide o Úrad Komisára pre vyšetrovacie právomoci, Európska komisia v odôvodnení 245 návrhu rozhodnutia vysvetľuje, že funguje ako nezávislý orgán, pričom je financovaný z prostriedkov ministerstva vnútra.

136. EDPB v návrhu rozhodnutia nenašiel ďalšie známky toho, že by bola posudzovaná nezávislosť Komisára pre uchovávanie a používanie biometrického materiálu a Komisára pre sledovanie kamerovým systémom.

137. **Európska komisia sa vyzýva, aby podrobnejšie posúdila nezávislosť Komisárov pre justíciu, a to aj v prípadoch, keď komisár (už) nevykonáva funkciu sudcu, a aby posúdila aj nezávislosť Komisára pre uchovávanie a používanie biometrického materiálu, ako aj Komisára pre sledovanie kamerovým systémom.**

4.2. Všeobecný právny rámec o ochrane údajov v oblasti národnej bezpečnosti

4.2.1. Osvedčenia o záujme národnej bezpečnosti

138. Podľa § 111 zákona o ochrane údajov z roku 2018 môžu prevádzkovatelia žiadať o osvedčenia o záujme národnej bezpečnosti [national security certificates], ktoré vydáva minister vlády, člen kabinetu, generálny prokurátor alebo generálny advokát v prípade Škótska a ktorými sa potvrdzuje, že výnimky zo záväzkov a práv zakotvených v časti 4 až 6 zákona o ochrane údajov z roku 2018 sú nevyhnutným a primeraným opatrením na ochranu národnej bezpečnosti. Účelom týchto osvedčení je poskytnúť prevádzkovateľom väčšiu právnu istotu a presvedčivo dokazujú skutočnosť, že pri spracúvaní osobných údajov sa uplatňuje hľadisko národnej bezpečnosti. Je potrebné uviesť, že tieto osvedčenia nie sú

potrebné na uplatnenie výnimiek v záujme národnej bezpečnosti, predstavujú skôr opatrenie transparentnosti[82].

139. EDPB pochopil z § 17 a 18 prílohy 20 k zákonu o ochrane údajov z roku 2018, že osvedčenie o záujme národnej bezpečnosti vydané na základe zákona o ochrane údajov z roku 1998 (ďalej len „staré osvedčenie") malo podľa zákona o ochrane údajov z roku 2018 predĺženú platnosť pre spracúvanie osobných údajov do 25. mája 2019. Do tohto dátumu sa so starými osvedčeniami, pokiaľ neboli vymenené alebo zrušené, zaobchádzalo tak, ako keby boli vydané podľa zákona o ochrane údajov z roku 2018.

140. Ale pokiaľ na osvedčení o záujme národnej bezpečnosti vydanom podľa zákona o ochrane údajov z roku 1998 nie je výslovne uvedený dátum skončenia platnosti, EDPB to chápe tak, že takéto osvedčenie bude naďalej platné vo vzťahu k spracúvaniu údajov podľa zákona o ochrane údajov z roku 1998, až pokým nebude odvolané alebo zrušené.[83] Hoci je ochrana poskytovaná týmito osvedčeniami obmedzená na spracúvanie osobných údajov podľa zákona o ochrane údajov z roku 1998, EDPB berie na vedomie, že nové osvedčenia o záujme národnej bezpečnosti sa môžu vydať podľa zákona o ochrane osobných údajov z roku 1998 pre osobné údaje spracúvané podľa tohto zákona.[84]

141. **Z dôvodu úplnosti EDPB vyzýva Európsku komisiu, aby vo svojom návrhu rozhodnutia objasnila, že osvedčenia o záujme národnej bezpečnosti sa môžu stále vydávať podľa zákona o ochrane údajov z roku 1998. Okrem toho EDPB vyzýva Európsku komisiu, aby vo svojom návrhu rozhodnutia opísala mechanizmy nápravy a dohľadu so zreteľom na osvedčenia vydávané podľa zákona o ochrane údajov z roku 1998. EDPB napokon Európsku komisiu vyzýva, aby do svojho návrhu rozhodnutia zahrnula počet existujúcich osvedčení vydaných podľa zákona o ochrane údajov z roku 1998 a tento aspekt pozorne monitorovala.**

4.2.2. Právo na opravu a právo na vymazanie

142. Pokiaľ ide o právo na opravu a právo na vymazanie, EDPB berie na vedomie, že v súlade s § 100 a § 149 zákona o ochrane údajov z roku 2018 majú dotknuté osoby možnosť obrátiť sa na Vrchný súd (najvyšší civilný súd pre Škótsko), aby prevádzkovateľ bez zbytočného odkladu opravil alebo vymazal ich údaje.

143. **EDPB zdôrazňuje, že sa musí účinne zabezpečiť uplatnenie práv dotknutých osôb; vyzýva preto Európsku komisiu, aby vo svojom návrhu rozhodnutia opísala, ako ustanovenia § 100 zákona o ochrane údajov z roku 2018 fungujú v praxi a aby úzko monitorovala uplatňovanie tohto paragrafu.**

4.2.3. Výnimky v záujme národnej bezpečnosti

144. Výbor by rád upozornil na § 110 zákona o ochrane údajov z roku 2018, a najmä prílohu 11, v ktorej sa stanovujú konkrétne účely, na ktoré sa môžu spravodajské služby odkloniť od určitých zásad ochrany údajov vrátane práv dotknutých osôb a v ktorých prípade nie sú povinní oznamovať porušenia ochrany osobných údajov ICO.[85]

---

[82] Pozri ministerstvo vnútra, zákon o ochrane údajov 2018, Usmernenie o osvedčeniach o záujme národnej bezpečnosti, august 2020, bod 4, s. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

[83] Pozri ministerstvo vnútra, zákon o ochrane údajov 2018, Usmernenie o osvedčeniach o záujme národnej bezpečnosti, august 2020, bod 4, s. 5.

[84] Pozri ministerstvo vnútra, zákon o ochrane údajov 2018, Usmernenie o osvedčeniach o záujme národnej bezpečnosti, august 2020, bod 8, s. 5.

[85] Týmito účelmi sú prechádzanie „trestnej činnosti" a jej odhaľovanie, „údaje, ktoré je podľa zákona

145. **EDPB vyzýva Európsku komisiu, aby ďalej objasnila rozsah pôsobnosti výnimiek, pretože si kladie otázku, či všetky výnimky poskytované v prílohe 11 k zákonu o ochrane údajov z roku 2018 sú relevantné pre prácu spravodajských služieb a či zabezpečujú zhodu so zásadami nevyhnutnosti a proporcionality**. **EDPB vyzýva Európsku komisiu, aby najmä poskytla ďalšie objasnenie o tom, za akých okolností sa môže spravodajská služba odvolávať na ustanovenia § 10 prílohy 11 v zákone o ochrane údajov z roku 2018, v ktorom sa stanovuje, že *„[u]vedené ustanovenia sa nevzťahujú na údaje, ktoré pozostávajú zo záznamov zámerov prevádzkovateľa v súvislosti s akýmikoľvek vyjednávaniami s dotknutou osobou v takom rozsahu, že by uplatnenie uvedených ustanovení pravdepodobne ohrozilo vyjednávania.“***

4.3. Prístup a používanie zo strany orgánov verejnej moci Spojeného kráľovstva na účely národnej bezpečnosti

146. EDPB vo všeobecnosti uznáva, že štátom sa udeľuje široká miera úvahy v otázkach národnej bezpečnosti, čo uznáva aj Európsky súd pre ľudské práva. EDPB zároveň pripomína, ako sa zdôrazňuje v jeho aktualizovaných odporúčaniach o európskych základných zárukách týkajúcich sa opatrení sledovania[86], že v článku 6 ods. 3 Zmluvy o Európskej únii sa stanovuje, že základné ľudské práva zakotvené v EDĽP tvoria všeobecné zásady právnych predpisov Únie. Ako však v rámci svojej jurisprudencie pripomína Súdny dvor EÚ, druhé uvedené netvorí bez pristúpenia EÚ k EDĽP právny nástroj formálne začlenený do právnych predpisov EÚ[87]. Úroveň ochrany základných práv požadovaná podľa článku 45 všeobecného nariadenia o ochrane údajov sa preto musí určiť na základe ustanovení tohto nariadenia, a to pri výklade so zreteľom na základné práva zakotvené v Charte EÚ. To znamená, že podľa článku 52 ods. 3 Charty EÚ práva v nej obsiahnuté, ktoré zodpovedajú právam zaručeným EDĽP, majú rovnaký význam a rozsah pôsobnosti ako práva stanovené v EDĽP. Preto, ako pripomína Súdny dvor EÚ, je potrebné zohľadniť jurisprudenciu Európskeho súdu pre ľudské práva v oblasti práv, ktoré sú zakotvené aj v Charte EÚ, ako minimálnu úroveň ochrany na výklad zodpovedajúcich práv v Charte EÚ[88]. Podľa poslednej vety článku 52 ods. 3 Charty EÚ však *„[t]oto ustanovenie nebráni právnym predpisom Únie v poskytovaní rozsiahlejšej ochrany.“*

147. V nasledujúcom posúdení preto EDPB zohľadnil jurisprudenciu Európskeho súdu pre ľudské práva v takom rozsahu, že Charta EÚ podľa výkladu Súdneho dvora Európskej únie nestanovuje vyššiu úroveň ochrany, ktorá predpisuje iné požiadavky ako judikatúra Európskeho súdu pre ľudské práva.

4.3.1. Právne základy, obmedzenia a záruky – vyšetrovacie právomoci uplatňované v kontexte národnej bezpečnosti

4.3.1.1. Všeobecné poznámky

148. EDPB pripomína, že zákon o vyšetrovacích právomociach z roku 2016 je nedávno prijatý zákon, ktorým sa mení viacero ustanovení zákona o spravodajských službách z roku 1994. Stanovuje sa

nevyhnutné sprístupniť alebo v súvislosti so súdnym konaním“, „parlamentné výsady“, „súdne konania“, „udelenie čestných titulov koruny“, „ozbrojené sily“, „hospodársky blahobyt“, „dôvernosť komunikácie medzi advokátom a jeho klientom“, „vyjednávania“, „dôverné údaje poskytnuté prevádzkovateľom“, „odpovede v písomných skúškach a známky zo skúšok“, „výskum a štatistika“ a „archivácia vo verejnom záujme“.

[86] Pozri odporúčania EDPB 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania.

[87] Pozri vec Schrems II, bod 98.

[88] Pozri Súdny dvor EÚ, spojené veci C-511/18, C-512/18 a C-520/18, La Quadrature du Net a ďalší, 6. október 2020, ECLI:EU:C:2020:791, bod 124.

v ňom, do akej miery sa môžu vyšetrovacie právomoci použiť na zásah do súkromia[89]. Napriek dvom správam Komisára pre vyšetrovacie právomoci, ktoré poskytujú užitočné informácie týkajúce sa uplatňovania tohto nového právneho rámca, stále nedošlo k preskúmaniu niektorých aspektov, najmä pokiaľ ide o výber použitých selektorov a kritérií vyhľadávania.

149. Pokiaľ ide o zákon o vyšetrovacích právomociach z roku 2016 a rozsah jeho uplatňovania vo všeobecnosti, EDPB zároveň zdôrazňuje štyri body, ktorým treba venovať pozornosť:

150. V súvislosti s **prvým bodom, ktorému treba venovať pozornosť,** pokiaľ ide o aspekty zákona, by EDPB rád zdôraznil dva aspekty:

151. EDPB v prvom rade poznamenáva, že tento právny predpis odkazuje na širšie účely použitia postupov stanovených v zákone o vyšetrovacích právomociach z roku 2016 a nie na kategórie jednotlivcov, ktorých sa týka získavanie údajov podľa častí 2 až 7 zákona o vyšetrovacích právomociach z roku 2016. EDPB v tejto súvislosti pripomína, že by na vymedzenie osobnej pôsobnosti zákona malo existovať prepojenie medzi kategóriami jednotlivcov, ktorí môžu byť predmetom opatrení sledovania, a účelmi, ktoré sleduje tento právny predpis.

152. Okrem toho EDPB zdôrazňuje, že vymedzenie pojmov „telekomunikační operátori", „telekomunikačné služby" a „telekomunikačný systém", ktorým sa vymedzuje rozsah pôsobnosti zákona, je do určitej miery takisto veľmi široké a nejasné. EDPB zdôrazňuje, že tieto pojmy v oblasti zákona o vyšetrovacích právomociach z roku 2016 sa musia v skutočnosti chápať značne širším spôsobom ako v právnych predpisoch upravujúcich telekomunikáciu, ako je vymedzené napríklad v európskom kódexe elektronických komunikácií[90]. EDPB berie na vedomie, že vymedzenia pojmov „telekomunikačná služba" a „telekomunikačný systém" v zákone sú navrhnuté zámerne širokým spôsobom tak, aby ostali relevantné pre nové technológie. Vymedzenie pojmu telekomunikačný operátor je podobne veľmi široké a mohlo by napríklad zahŕňať online videohry s funkciou posielania správ alebo iné webové sídla, ktoré obsahujú takéto okná na posielanie správ[91].

153. Okrem toho, kým postupy a dohľad týkajúci sa posúdenia nevyhnutnosti a proporcionality získavania údajov a prístupu k nim sú vo všeobecnosti stanovené, kritériá pristúpenia k takémuto posúdeniu nie sú v zákone samom osebe vymedzené. Dodatočné prvky sú uvedené v ďalších dokumentoch, napríklad v Kódexoch postupov.

154. Ako sa však pripomína v odporúčania EDPB 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania, Súdny dvor EÚ naznačil, že *„požiadavka, podľa ktorej musí byť každé obmedzenie výkonu základných práv stanovené zákonom* [law]*, predpokladá, že samotný právny základ, ktorý umožňuje zásah do týchto práv, musí vymedzovať rozsah obmedzenia výkonu dotknutého práva."*[92] Presnejšie Súdny dvor EÚ objasnil, že *„[n]a účely splnenia požiadavky proporcionality musí právna úprava stanoviť jasné a presné pravidlá, ktoré budú*

[89] Pozri § 1 zákona o vyšetrovacích právomociach z roku 2016.

[90] Pozri článok 2 ods. 5 európskeho kódexu elektronických komunikácií, v ktorom sa napríklad vymedzuje „interpersonálna komunikačná služba" ako *„ služba obvykle poskytovaná za odplatu, ktorá umožňuje priamu interpersonálnu a interaktívnu výmenu informácií prostredníctvom elektronických komunikačných sietí medzi konečným počtom osôb, pričom osoby, ktoré komunikáciu začali alebo sa na nej zúčastňujú, určujú jej prijímateľa(-ľov) a nezahŕňa služby, ktoré umožňujú interpersonálnu a interaktívnu komunikáciu len ako vedľajšiu doplnkovú zložku neoddeliteľne spojenú s inou službou."*

[91] Pozri ministerstvo vnútra, Kódex postupov pre zachytávanie komunikácie, marec 2018, odseky 2.5 a ďalšie, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Pozri vec Schrems II, bod 175, a uvedená judikatúra, ako aj rozsudok Súdneho dvora Európskej únie, vec C-623/17 Privacy International/Secretary of State for Foreign and Commonwealth Affairs, 6. októbra 2020, ECLI:EU:C:2020:790 (ďalej len „Privacy International"), bod 65.

upravovať rozsah a uplatnenie predmetného opatrenia a ukladať minimálne požiadavky tak, aby osoby, ktorých údaje boli prenesené, mali dostatočné záruky umožňujúce im účinne chrániť ich osobné údaje pred rizikami zneužitia. Táto právna úprava musí byť podľa vnútroštátneho práva právne záväzná a musí najmä vymedziť okolnosti a podmienky, za akých možno prijať opatrenie upravujúce spracúvanie takýchto údajov, čím zaručí, aby zásah nešiel nad rámec toho, čo je striktne nevyhnutné."[93]

155. Európsky súd pre ľudské práva takisto zdôraznil význam jasnosti práva, ktoré jednotlivcom poskytuje *„primerané informácie, pokiaľ ide o okolnosti a podmienky, za akých majú orgány verejnej moci právomoc využiť ktorékoľvek z týchto opatrení."*[94]

156. **EDPB preto vyzýva Európsku komisiu, aby ďalej posúdila tieto aspekty týkajúce sa presnosti, jasnosti a úplnosti príslušných právnych predpisov a aby poskytla ďalšie prvky, ktoré preukazujú, že poskytujú úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany poskytovanej v rámci Únie, pokiaľ ide o aspekty právnych predpisov. Výbor zároveň zdôrazňuje, že široké vymedzenia by sa mali takisto posúdiť vo vzťahu k proporcionalite opatrení na zachytávanie.**

157. Hoci sa vo viacerých interných kódexoch príslušných orgánov spravodajského spoločenstva čiastočne vypracovali niektoré z týchto prvkov, napríklad pokiaľ ide o posúdenie nevyhnutnosti a proporcionality získavania údajov, EDPB zároveň zdôrazňuje, že požiadavky Súdneho dvora EÚ v súvislosti s povahou právnych predpisov znamenajú, že kľúčové prvky vrátane tých, ktoré jednotlivcom umožňujú ich využitie v kontexte nápravy, sa musia zabezpečiť v právnych predpisoch, v ktorých sa stanovujú uplatniteľné práva.[95] V § 6 prílohy 7 k zákonu o vyšetrovacích právomociach z roku 2016 sa skutočne uvádza, že súdy (a dozorné orgány) *„zohľadnia nesplnenie osoby, pokiaľ ide o povinnosť dodržiavať kódex pri určovaní odpovede na otázku v akomkoľvek z týchto postupov"* bez toho, aby sa objasnilo, či jednotlivci môžu uplatniť porušenie kódexu pred súdmi (alebo dozornými orgánmi). Okrem toho sa v doteraz uvedených prvkoch návrhu rozhodnutia uvádza uznanie Európskeho súdu pre ľudské práva týkajúce sa skôr predvídateľnosti pravidiel stanovených v týchto kódexoch[96] ako ich „uplatniteľnosti" pred súdom tak, ako to požaduje Súdny dvor EÚ, alebo skutočnosť, že súdne orgány Spojeného kráľovstva v niektorých prípadoch odkazovali na kódexy, pričom ani jeden z uvedených prípadov nepoukazuje na možnosť jednotlivcov uplatňovať práva vyplývajúce z kódexov. **Ak sa dospeje k záveru, že právne predpisy Spojeného kráľovstva v dostatočnej miere neuvádzajú okolnosti a podmienky, za akých možno opatrenie prijať a že sa tieto prvky v skutočnosti stanovujú v interných kódexoch orgánov spravodajského spoločenstva, EDPB preto vyzýva Európsku komisiu, aby ďalej posúdila, či si môžu jednotlivci uplatniť obmedzenia a záruky stanovené v rôznych interných kódexoch orgánov spravodajského spoločenstva pred súdmi a či sa môžu presadzovať.**

[93] Pozri vec Privacy International, bod 68.

[94] Pozri Európsky súd pre ľudské práva, *Z*akharov/Ruská federácia, 4. decembra 2015, CE:ECHR:2015:1204JUD004714306, bod 229.

[95] V tejto súvislosti Súdny dvor EÚ vzal do úvahy, že napríklad prezidentská politická smernica (PPD 28) USA nespĺňa podmienky napriek tomu, že sa v nej stanovujú niektoré obmedzenia týkajúce sa hromadného získavania, pozri vec Schrems II, bod 181.

[96] Pozri Európsky súd pre ľudské práva, Big Brother Watch and others/Spojené kráľovstvo Veľkej Británie a Severného Írska, 13. septembra 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (ďalej len „Big Brother Watch"), bod 325: *„Keďže Kódex postupov pre zachytávanie komunikácie je verejným dokumentom vyžadujúcim schválenie obidvomi snemovňami parlamentu a musia ho zohľadňovať osoby vykonávajúce úlohy v oblasti zachytávania aj súdy a tribunály, súd výslovne pripúšťa, že jeho ustanovenia by sa mohli zohľadňovať pri posúdení predvídateľnosti režimu zákona o regulácii vyšetrovacích právomocí."*

158. **Druhý bod, ktorému treba venovať pozornosť**, sa týka skutočnosti, že ustanovenia vzťahujúce sa na jednej strane na cielené získavanie a uchovávanie údajov o komunikácii a na strane druhej na hromadné získavanie, či už v zákone o vyšetrovacích právomociach z roku 2016 alebo v iných právnych predpisoch, ako sú zákon o spravodajských službách z roku 1994 alebo zákon o regulácii vyšetrovacích právomocí z roku 2000, sa budú uplatňovať aj na údaje prenášané z EÚ do Spojeného kráľovstva. Pokiaľ ide o hromadné získavanie, EDPB zdôrazňuje, že príslušné ustanovenia právnych predpisov Spojeného kráľovstva umožňujú získavanie údajov mimo Spojeného kráľovstva; mohlo by preto obsahovať údaje v tranzite prenášané z EHP do Spojeného kráľovstva na základe rozhodnutia o primeranosti.[97] EDPB okrem toho zaznamenáva, že Európska komisia uviedla, že *„je potrebné poznamenať, že uchovávanie a získavanie údajov o komunikácii sa zvyčajne netýka osobných údajov dotknutých osôb z EÚ prenesených do Spojeného kráľovstva na základe tohto rozhodnutia. Povinnosť uchovávať alebo poskytnúť údaje o komunikácii podľa časti 3 a 4 zákona o vyšetrovacích právomociach z roku 2016 sa vzťahuje na údaje, ktoré sú získavané telekomunikačnými operátormi v Spojenom kráľovstve priamo od používateľov telekomunikačných služieb.“*[98] EDPB však zdôrazňuje nedostatok jasnosti týkajúcej sa skutočnosti, že len zariadenia týchto operátorov so sídlom v Spojenom kráľovstve môžu dostávať žiadosti od príslušných orgánov Spojeného kráľovstva, keďže podľa vymedzenia pojmu telekomunikačný operátor stanoveného v § 261 ods. 10 zákona o vyšetrovacích právomociach z roku 2016 sa vyžaduje, že „telekomunikačný operátor je osoba, ktorá ponúka alebo poskytuje telekomunikačné služby osobám v Spojenom kráľovstve *alebo ktorá poskytuje telekomunikačný systém, ktorý sa (úplne alebo čiastočne) nachádza v Spojenom kráľovstve, alebo ho prevádzkuje.“* Na osobné údaje dotknutých osôb v EHP by sa to mohlo vzťahovať napríklad v prípade získavania alebo vytvárania údajov zariadením telekomunikačného operátora Spojeného kráľovstva na území EHP, ktoré sú prenášané do zariadenia toho istého operátora na území Spojeného kráľovstva na základe rozhodnutia o primeranosti (na komerčné účely) a následne získavané v rámci Spojeného kráľovstva príslušnými orgánmi verejnej moci.

159. **EDPB je preto toho názoru, že posúdenie týchto ustanovení je zároveň relevantné pre posúdenie úrovne primeranosti právneho rámca Spojeného kráľovstva a vyzýva Európsku komisiu, aby objasnila tento aspekt a ďalej posúdila, do akej miery to zodpovedá skutočnosti. Konkrétne EDPB Európsku komisiu vyzýva, aby objasnila svoje chápanie rozsahu pôsobnosti týchto právnych predpisov vrátane toho, na čo sa vzťahuje pojem „používatelia telekomunikačných služieb“, a či možno vzhľadom na veľmi široké vymedzenie telekomunikačných operátorov žiadať o údaje zo zariadení telekomunikačných operátorov so sídlom mimo Spojeného kráľovstva v rozsahu, ktorý by sa vzťahoval na údaje dotknutých osôb v EHP.**

160. **Tretí bod, ktorému treba venovať pozornosť**, sa týka tzv. postupu dvojitého zabezpečenia. EDPB berie na vedomie, že nový postup dvojitého zabezpečenia bol zavedený v zákone o vyšetrovacích právomociach z roku 2016. EDPB však chápe, že aj ak by sa v zásade získavanie údajov a prístup k nim na účely národnej bezpečnosti a spravodajské účely odohrávalo na základe príkazu schváleného Komisárom pre justíciu, v zákone o vyšetrovacích právomociach z roku 2016 sa stanovuje, že *„v konkrétnych obmedzených prípadoch je možné zákonné zachytávanie bez príkazu a potrebné je len predchádzajúce povolenie príslušných orgánov spravodajského spoločenstva [pozri ďalej oddiel o dohľade] vrátane zachytávania v súlade so zahraničnými žiadosťami (§ 52 zákona o vyšetrovacích právomociach z roku 2016.).“* Ako sa ďalej zdôrazňuje, potvrdzuje to takisto obavy EDPB, najmä pokiaľ ide o poskytovanie údajov do zahraničia. EDPB okrem toho berie na vedomie, že v súvislosti so zasahovaním do zariadení, či

[97] Pozri bod 183 a ďalšie vo veci Schrems II o posúdení právnych predpisov, ktorými sa umožňuje prenos údajov v tranzite medzi EÚ a treťou krajinou v kontexte rozhodnutia o primeranosti.
[98] Pozri odôvodnenie 196 návrhu rozhodnutia.

už cieleným alebo hromadným, takisto existuje možnosť odchýlky od postupu dvojitého zabezpečenia a že Komisár pre justíciu je oprávnený povoliť len obnovu hromadných príkazov po uplynutí prvého obdobia najviac 6 mesiacov. **EDPB vyzýva Európsku komisiu, aby ďalej posúdila a preukázala, že právny rámec Spojeného kráľovstva stanovuje primerané záruky aj v prípadoch, v ktorých sa neuplatňuje postup dvojitého zabezpečenia, vrátane účinného dohľadu *ex post* a možností nápravy poskytované jednotlivcom tak, aby sa zabezpečila úroveň ochrany, ktorá je v podstate rovnocenná s úrovňou ochrany poskytovanou v EÚ (pozri ďalej oddiel 4.3.3. o dohľade).**

161. Okrem toho, hoci sa zákonom o vyšetrovacích právomociach z roku 2016 skutočne zavádza postup dvojitého zabezpečenia, EDPB je naďalej znepokojený v súvislosti s určitými aspektmi nového právneho predpisu. Po predstavení zodpovedajúcich oddielov návrhu rozhodnutia EDPB analyzoval tieto druhy získavania údajov a prístupu k nim v rovnakom poradí, ako boli predstavené Európskou komisiou. Poradie ďalej posudzovaných prvkov preto neodzrkadľuje hierarchiu, pokiaľ ide o úroveň znepokojenia zo strany EDPB.

4.3.1.2. Cielené získavanie a uchovávanie údajov o komunikácii

162. EDPB poznamenáva, že existujú dvaja verejní činitelia, ktorí môžu udeľovať cielené povolenia na získanie údajov o komunikácii: povoľujúci úradník Úradu pre povolenia o údajoch o komunikácii (ďalej len „Komisár pre vyšetrovacie právomoci“), určený vyšší úradník (osoba vykonávajúca funkciu alebo hodnosť príslušného orgánu verejnej moci), spolu s povolením Komisára pre justíciu v určitých prípadoch. EDPB však naďalej nie je jasné, ktorý úradník podľa zákona a príslušného kódexu presne povoľuje ktorý druh cieleného získavania údajov o komunikácii a do akej miery by bol určený úradník dostatočne nezávislý.[99]

163. **EDPB preto vyzýva Európsku komisiu, aby ďalej posúdila tento aspekt a poskytla jasnejšie vysvetlenia týkajúce sa týchto prvkov.**

164. Pokiaľ ide o príkaz vyžadujúci uchovávanie údajov o komunikácii, EDPB zároveň poznamenáva, že takého príkazy sa môžu vydať „opisu operátorov“. Mohlo by sa javiť, že tento pojem znamená možnosť požiadať niekoľkých operátorov o to, aby uchovávali údaje. Cielený charakter získavania sa v skutočnosti nevzťahuje na počet operátorov, ale na mená alebo opis osôb, organizácií, polohy alebo skupiny osôb, ktoré predstavujú „cieľ“, opis podstaty vyšetrovania a opis činností, na ktoré sa zariadenie využíva. EDPB preto zdôrazňuje, že v závislosti od počtu dotknutých operátorov, na ktorých sa vzťahuje takýto „opis operátorov“, môže mať príkaz širšiu povahu, ako by mohlo vyplývať z postupu cieleného zachytávania. **EDPB vyzýva Európsku komisiu, aby ďalej posúdila tento aspekt a poskytla ďalšie záruky, že aj ak sa príkazy vydávajú viacerým operátorom, ostávajú obmedzené na to, čo je striktne nevyhnutné a primerané.**

4.3.1.3. Zasahovanie do zariadení

165. EDPB poznamenáva, že „zasahovanie do zariadení“ sa môže v prípade naliehavých dôvodov odkloniť od postupu dvojitého zabezpečenia.[100] EDPB preto vyjadruje obavy, že účely, na ktoré sa môže požadovať takéto zasahovanie do zariadení, sú široké a že kritériá naliehavých dôvodov (v ktorom sa nevyžaduje poskytnutie *ex ante* povolenia Komisárom pre justíciu po vykonaní posúdenia nevyhnutnosti a proporcionality zasahovania do zariadení) ostávajú nejasné. Keďže v druhej uvedenej situácii „príkazy strácajú svoj vplyv a nemôžu byť obnovené“ za predpokladu, že Komisár pre justíciu neschváli

[99] Pozri ďalej oddiel o posúdenia postupu dvojitého zabezpečenia a nezávislosti Komisára pre justíciu.
[100] Pozri § 109 zákona o vyšetrovacích právomociach z roku 2016.

zasahovanie do zariadení *ex post*, EDPB to chápe tak, že medzitým získané údaje ostávajú právoplatne získané. Na vymazanie týchto údajov môže Komisár pre justíciu vydať osobitný príkaz.[101]

166. **EDPB vyzýva Európsku komisiu, aby ďalej posúdila podmienky, za ktorých sa možno odvolávať na naliehavé dôvody a aby poskytla objasnenia týkajúce sa dostupných prostriedkov na uplatňovanie práv dotknutých osôb a dostupných prostriedkov nápravy, ktoré môžu využiť v kontexte operácií zasahovania do zariadení, predovšetkým ak sa uskutočňujú v kontexte naliehavých dôvodov, čo vedie k odchýlke od postupu dvojitého zabezpečenia.**

4.3.1.4. Hromadné zachytávanie údajov od nositeľov

167. Ako sa uvádza v správe o preskúmaní hromadných právomocí[102], *„[h]romadné zachytávanie zvyčajne pozostáva zo získavania komunikácií pri ich tranzite konkrétnymi nositeľmi (komunikačné prepojenia).“* V oficiálnom prehľade týkajúcom sa zákona o vyšetrovacích právomociach z roku 2016 sa opisuje „hromadné zachytávanie“ ako *„postup získavania objemu komunikácií, po ktorom nasleduje výber konkrétnych komunikácií, ktoré sa čítajú, prezerajú alebo počúvajú tam, kde je to nevyhnutné a primerané.“* EDPB berie na vedomie, že „hromadné zachytávanie“ údajov v skutočnosti znamená získavanie údajov ešte pred akýmkoľvek filtrovaním selektormi (či už ide o jednoduché filtrovanie v kontexte monitorovania už známych jednotlivcov, ktorí predstavujú hrozbu, alebo komplexné filtrovanie v kontexte identifikácie nových hrozieb alebo doposiaľ neznámych osôb záujmu).

168. Získavanie hromadných údajov o komunikácii takisto predstavovalo jednu z otázok, ktorú preskúmal Súdny dvor EÚ vo veci Privacy International, ktorej výsledkom je rozsudok veľkej komory vydaný 6. októbra 2020 (okrem toho, či sa toto získavanie údajov vykonávalo v kontexte právnych predpisov EÚ, a to aj na účely národnej bezpečnosti). Zákon o vyšetrovacích právomociach z roku 2016 nahradil právne predpisy, ktoré boli predmetom tohto rozsudku.

169. EDPB poznamenáva, že po zavedení zákona o vyšetrovacích právomociach z roku 2016 do právnych predpisov Spojeného kráľovstva je v súčasnosti potrebný príkaz aj na hromadné zachytávanie údajov. Postup vydávania tohto príkazu spočíva v určení „operačných účelov“. Zoznam týchto operačných účelov zostavujú vedúci spravodajských služieb a následne ho schvaľuje minister. Toto rozhodnutie samo osebe schvaľuje nezávislý Komisár pre justíciu, ktorý musí preskúmať, či je príkaz nevyhnutný a primeraný na operačné účely. EDPB chápe, že Komisár pre justíciu nemá právomoc posúdiť operačné účely samy osebe, ale to, či je príkaz nevyhnutný a primeraný na operačné účely uvedené v príkaze. Parlamentnému výboru pre spravodajstvo a bezpečnosť sa predkladá kópia zoznamu každé tri mesiace a predseda vlády preskúmava zoznam týchto operačných účelov najmenej raz ročne.

170. Na základe prvkov predložených Európskou komisiou v návrhu rozhodnutia sa však zdá náročné posúdiť rozsah pôsobnosti týchto operačných účelov obsiahnutých na zozname a to, či získavanie údajov, ktoré umožňujú, spĺňa úroveň stanovenú Súdnym dvorom Európskej únie (napríklad vymedzenie získavania údajov na zemepisnú oblasť veľkosti niekoľkých ulíc, ako aj získavanie údajov z EHP ako celku).

171. EDPB okrem toho zdôrazňuje, že hromadne získané údaje sa môžu uchovávať na dlhšie obdobie (aby boli prístupné na ďalšie preskúmanie). EDPB pripomína, že v § 150 ods. 5 a 6 zákona o vyšetrovacích právomociach z roku 2016 sa stanovuje iba zničenie kópií získaných údajov, a to iba v prípade, ak ich uchovávanie nie je nevyhnutné alebo ak nie je pravdepodobné, že sa stane nevyhnutné, v záujme národnej bezpečnosti alebo na základe akéhokoľvek dôvodu, ktorý patrí do rozsahu pôsobnosti § 138

[101] Pozri § 110, pododdiel 3 písm. b) zákona o vyšetrovacích právomociach z roku 2016.
[102] Pozri Správu o preskúmaní hromadných právomocí nezávislým revízorom právnych predpisov v oblasti boja proti terorizmu, august 2016.

ods. 2 zákona o vyšetrovacích právomociach z roku 2016, alebo ak ich uchovávanie nie je nevyhnutné na viacero iných účelov.[103] EDPB poznamenáva, že tieto dôvody sa zdajú veľmi široké a v každom prípade sa uvádzajú len kópie získaných údajov.

172. Okrem toho EDPB poznamenáva, že v naliehavých prípadoch ustanovenia zákona o vyšetrovacích právomociach z roku 2016 umožňujú zmenu príkazov bez predchádzajúceho schválenia Komisárom pre justíciu a v takom prípade, ak Komisár pre justíciu, s ktorým sa konzultuje *ex post*, do troch pracovných dní od úpravy odmietne zmenu schváliť, príkaz má taký účinok, ako by sa zmena nevykonala, medzitým získané údaje však ostávajú právoplatne získané.[104] Na vymazanie týchto údajov môže Komisár pre justíciu vydať osobitný príkaz.[105]

173. **EDPB preto vyzýva Európsku komisiu, aby ďalej objasnila a posúdila hromadné zachytávania, najmä pokiaľ ide o výber a uplatňovanie selektorov v kontexte týchto postupov hromadného zachytávania, aby sa objasnilo, do akej miery prístup k osobným údajom spĺňa úroveň stanovenú Súdnym dvorom EÚ (pozri aj ďalej uvedený oddiel 4.3.1.7., najmä čo sa týka dohľadu nad selektormi) a aké záruky sú zavedené na ochranu základných práv jednotlivcov, ktorých údaje sa zachytávajú v tomto kontexte vrátane období uchovávania údajov. Mimoriadne užitočné by bolo nezávislé posúdenie zo strany príslušných orgánov dohľadu Spojeného kráľovstva.**

174. **EDPB zároveň zdôrazňuje, že ešte dôležitejšie sa zdá byť to, že „zahraničná komunikácia", ktorá patrí do rozsahu postupov hromadného zachytávania, naznačuje, že Spojené kráľovstvo by mohlo údaje priamo hromadne zachytávať a získavať na území EHP vrátane údajov v tranzite medzi EHP a Spojeným kráľovstvom, ktoré by patrilo do rozsahu pôsobnosti návrhu rozhodnutia (pozri oddiel 4.3.2. o ďalšom používaní získaných informácií na účely národnej bezpečnosti a poskytovaní údajov do zahraničia).**

4.3.1.5. Ochrana a záruky týkajúce sa sekundárnych údajov

175. Okrem toho je EDPB znepokojený tým, že sa v príslušných právnych predpisoch Spojeného kráľovstva týkajúcich sa hromadného zachytávania nestanovuje rovnaká úroveň ochrany pre všetky údaje o komunikácii. „Sekundárne údaje", ktoré sa môžu získať v rámci hromadného príkazu predstavujú podľa § 137 zákona o vyšetrovacích právomociach z roku 2016 tak „systémové informácie", *„ktoré sú obsiahnuté v rámci komunikácie ako jej súčasť, sú k nej pripojené alebo logicky s ňou súvisia (či už s odosielateľom alebo nie),"* ako aj „identifikačné údaje", *„ktoré sú obsiahnuté v rámci komunikácie ako jej súčasť, sú k nej pripojené alebo logicky s ňou súvisia (či už s odosielateľom alebo nie), môžu sa logicky oddeliť od ostatnej komunikácie alebo informácie a ak by sa takto oddelili, neodhalili by nič, čo možno odôvodnene považovať za zmysel (ak nejaký existuje) komunikácie alebo informácie, a to bez ohľadu na akýkoľvek zmysel vyplývajúci zo skutočnosti komunikácie alebo z akýkoľvek údajov týkajúcich sa prenosu komunikácie."*[106]

176. EDPB poznamenáva, že na tieto hromadne získavané „sekundárne údaje", známe aj ako „metaúdaje"[107], sa nevzťahujú rovnaké záruky ako na údaje získané cieleným príkazom, ale ani ako hromadne získavané obsahové údaje. EDPB poznamenáva, že na výber akéhokoľvek zachyteného obsahu sa vzťahuje viac záruk[108] ako výber sekundárnych údajov.[109]

[103] Pozri pododdiely 3 a 6 § 150 zákona o vyšetrovacích právomociach z roku 2016.
[104] Pozri § 147 zákona o vyšetrovacích právomociach z roku 2016 (časť 6 kapitola I).
[105] Pozri § 181, pododdiel 3 písm. b) zákona o ochrane údajov z roku 2016.
[106] „Systémové údaje" a „identifikačné údaje" sa vymedzujú v § 263 zákona o vyšetrovacích právomociach z roku 2016.
[107] Pozri Správu o preskúmaní hromadných právomocí nezávislým revízorom právnych predpisov v oblasti boja proti terorizmu, august 2016.
[108] Pozri § 152, pododdiel 1 písm. c) a pododdiely 3 a ďalšie zákona o vyšetrovacích právomociach z roku 2016.
[109] Pozri § 152, pododdiel 1 písm. a) a b) zákona o vyšetrovacích právomociach z roku 2016.

177. EDPB navyše zdôrazňuje, Európsky súd pre ľudské práva[110] aj Súdny dvor EÚ[111] spochybnili skutočnosť, že takéto údaje sú menej citlivé v porovnaní s inými druhmi údajov, a najmä v porovnaní s obsahovými údajmi. V kódexe postupov pre zachytávanie sa vskutku uvádzajú príklady „sekundárnych údajov" („systémových údajov", ako sú nastavenia routera, e-mailové adresy alebo ID používateľov; ale aj alternatívne identifikátory účtu, ako aj „identifikačných údajov", ako sú miesto stretnutia uložené v kalendári, informácie o fotografiách, napr. čas, dátum a miesto jej vytvorenia). **EDPB preto zdôrazňuje konzistentné posúdenie Európskeho súdu pre ľudské práva a Súdneho dvora Európskej únie a pripomína obavy vyjadrené v súvislosti so sekundárnymi údajmi, na ktoré by sa mali vzťahovať osobitné záruky z dôvodu ich citlivosti**. **EDPB preto vyzýva Európsku komisiu, aby starostlivo posúdila, či sa zárukami stanovenými v rámci právnych predpisov Spojeného kráľovstva pre túto kategóriu osobných údajov zabezpečuje v podstate rovnocenná úroveň ochrany, aká je zaručená v EÚ.**

4.3.1.6. Automatizované spracúvanie údajov o komunikácii

178. EDPB berie na vedomie, že orgány spravodajského spoločenstva [intelligence community authorities] nepoužívajú jednoduché alebo komplexné selektory na filtrovanie hromadne získaných údajov, ale že môžu podľa správy Výboru pre spravodajstvo a bezpečnosť z roku 2015[112] využiť aj iné nástroje automatického spracúvania na analýzu *„veľkého objemu informácií, čo agentúram umožňuje odhaľovať spojenia, vzorce, pridruženia alebo správania, ktoré by mohli poukazovať na závažné ohrozenie, ktoré si vyžaduje vyšetrovanie."* **EDPB si uvedomuje skutočnosť, že táto verejná správa sa týka postupov v rámci predchádzajúceho právneho rámca, ktorý nahradil zákon o vyšetrovacích právomociach z roku 2016. Vidí však potrebu ďalšieho posúdenia používania nástrojov automatizovaného spracúvania a dohľadu nad nimi kompetentnými dozornými orgánmi Spojeného kráľovstva, pričom vyzýva Európsku komisiu, aby ďalej posúdila túto otázku a záruky, ktoré by v tejto súvislosti mohli a/alebo mali byť poskytované dotknutým osobám v EHP.**

[110] Pozri rozsudok ESĽP, Big Brother Watch, bod 357 v odvolaní na veľkú komoru: *„Hoci Súd nespochybňuje, že príslušné údaje o komunikácii sú základným nástrojom pre spravodajské služby v boji proti terorizmu a závažnej trestnej činnosti, domnieva sa preto, že orgány ich úplným vyňatím zo záruk uplatniteľných na vyhľadávanie a preskúmavanie obsahu nedosahujú spravodlivé vyváženie medzi verejným a súkromným záujmom. Hoci Súd nenavrhuje, aby boli príslušné údaje o komunikácii prístupné len na účely určenia, či sa jednotlivec nachádza na území Britských ostrovov, keďže by si to vyžadovalo uplatňovanie prísnejších noriem na príslušné údaje o komunikácii ako na obsah, mali by však byť zavedené dostatočné záruky, ktorými sa zabezpečuje, že sú výnimky príslušných údajov o komunikácii z požiadaviek § 16 zákona o regulácii vyšetrovacích právomocí obmedzené v rozsahu nevyhnutnom na určenie, či sa jednotlivec v tom čase nachádza na Britských ostrovoch."*

[111] Pozri rozsudok Súdny dvor Európskej únie, vec Privacy International, bod 71: *„Zásah do práva zakotveného v článku 7 Charty, ktorý spôsobuje odovzdávanie údajov o prenose dát a polohe* [traffic data and location data] *bezpečnostným a spravodajským službám, treba považovať za obzvlášť závažný najmä vzhľadom na citlivú povahu informácií, ktoré môžu z týchto údajov vyplynúť, a najmä možnosť vytvoriť z nich profily dotknutých osôb, pričom takáto informácia je rovnako citlivá ako samotný obsah komunikácie. Navyše môže v povedomí dotknutých osôb vyvolať pocit, že ich súkromný život je predmetom neustáleho sledovania (pozri analogicky rozsudky z 8. apríla 2014, Digital Rights Ireland a i., C-293/12 a C-594/12, EU:C:2014:238, body 27 a 37, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 99 a 100)."*

[112] Pozri Parlamentný výbor pre spravodajstvo a bezpečnosť, Súkromie a bezpečnosť: moderný a transparentný právny rámec, 2015, § 18, s. 13 https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

4.3.1.7. Riziko nedodržania súladu s predpismi a postupy orgánov spravodajského spoločenstva, ktoré nie sú v súlade predpismi

179. EDPB berie na vedomie, že sú dostupné podrobné správy týkajúce sa dohľadu. Poskytujú sa v nich cenné príspevky, pokiaľ ide o to, čo posudzujú ako pozitívne postupy v súlade s predpismi, ako aj riziká nedodržania súladu s predpismi a určené postupy, ktoré nie sú v súlade s predpismi.

180. Podľa správy Komisára pre vyšetrovacie právomoci z roku 2019 sa v tejto súvislosti vo viacerých prvkoch týkajúcich sa uplatňovania právneho rámca rôznymi príslušnými orgánmi odhalili niektoré prípady (alebo riziká) nesúladu príslušných orgánov.

181. Po prvé, EDPB zaznamenal, že kritériá na označenie súboru údajov za súbor hromadných osobných údajov alebo ako cielené údaje nie sú vždy jasné pre Bezpečnostnú službu (MI5) a Tajnú spravodajskú službu (SIS), najmä pre Bezpečnostnú službu (MI5), čo môže viesť k absencii primeraných záruk uplatňovaných na údaje.[113] V tejto správe z roku 2019 Komisár pre vyšetrovacie právomoci navrhol, že *„táto otázka by sa mala prioritne vyriešiť.“*[114] Aj pokiaľ ide o Vládne komunikačné ústredie, EDPB v súvislosti so súbormi hromadných osobných údajov poznamenáva, že hoci klasifikácia súborov hromadných osobných údajov sa zdá uspokojivá (aj keď stále čaká na vykonanie auditu Komisárom pre vyšetrovacie právomoci), z interného preskúmania dodržiavania postupov v príkazoch, ktoré vykonala špecializovaná skupina v marci 2019, vyplýva vážne znepokojenie, pričom 50 % odôvodnení príkazov na hromadné získavanie, ktoré preskúmala skupina na posúdenie dodržiavania súladu Vládnym komunikačným ústredím, nedosahovalo požadovanú úroveň. Podľa Komisára pre vyšetrovacie právomoci začala skupina práce na preskúmaní problému a preškolení zamestnancov s cieľom zlepšiť túto úroveň. Aktualizačná odborná príprava o ustanoveniach zákona o vyšetrovacích právomociach z roku 2016 a ďalšia odborná príprava poskytované sieťami pre politiku a dodržiavanie (ďalej len „PCN“) zlepšili úroveň dodržiavania Vládneho komunikačného ústredia v tejto oblasti. Komisár pre vyšetrovacie právomoci neočakáva nedostatky týkajúce sa tejto úrovne pri budúcich kontrolách, bude však naďalej úzko preskúmavať túto oblasť.[115] **EDPB preto súhlasí s názorom, že ďalšie preskúmanie a monitorovanie uvedených prvkov Európskou komisiou je potrebné ako súčasť posúdenia úrovne ochrany, aby sa zabezpečilo zlepšenie tejto úrovne, ako sa zdôrazňuje v správe Komisára pre vyšetrovacie právomoci, a pripomína, že vykonávanie a konkrétne uplatňovanie právneho rámca by sa malo rovnako zohľadniť pri posudzovaní podstatnej rovnocennosti tretej krajiny, ako sa stanovuje v článku 45 všeobecného nariadenia o ochrane údajov.**

[113] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: *„Pozorovali sme pozitívny vývoj [Panel pre dohľad na hromadnými údajmi (Bulk Oversight Panel BOP)] a berieme na vedomie jeho vplyv na riadenie vnútorného dodržiavania. Ďalšie objasnenia žiadame v súvislosti s postupom, ktorý Bezpečnostná služba (MI5) používa na vykonávanie prvotných preskúmavaní nových súborov údajov s cieľom lepšie porozumieť rozhodnutiam označiť súbor údajov za súbor hromadných osobných údajov alebo napríklad za cielené údaje. Znepokojilo nás jedno nevyriešené opatrenie zo zápisnice panelu BOP týkajúce sa riešenia nezrovnalostí medzi prideľovaním súborov hromadných osobných údajov medzi Bezpečnostnou službou (MI5) a Tajnou spravodajskou službou (SIS). Je pravdepodobné, že obe agentúry mohli z dôvodu odlišného použitia a diferencovania uchovávaných údajov uchovávať rovnaký súbor údajov, alebo jeho verzie, a že sa mohol zákonne kategorizovať ako hromadný súbor jednou agentúrou a ako cielené údaje druhou agentúrou. Existuje riziko, že ak jedna z agentúr nesprávne kategorizovala uchovávané údaje ako cielené, môžu sa tieto údaje uchovávať bez príslušného príkazu a nemusia byť predmetom primeraných záruk.“*
[114] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 8.39.
[115] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.48.

182. EDPB v širšom zmysle zdôrazňuje dôležité body uvedené Komisárom pre vyšetrovacie právomoci, ktoré sa týkajú „vyhľadávaní založených na úlohe“ vykonávaných príslušníkmi Bezpečnostnej služby (MI5) a ktoré umožňujú vyšetrovateľom vykonávanie viacnásobného vyhľadávania v dostupných súboroch hromadných osobných údajov, ako aj *„závažných rizík nedodržania súladu s predpismi súvisiacich s konkrétnymi prostrediami technológií používaných Bezpečnostnou službou (MI5)“*, ktoré sa týkajú toho, kde boli údaje v rámci prostredia uschované, kto mal k nim prístup, do akej miery boli kopírované alebo ďalej poskytované, postupy ich vymazávania, ako aj období ich uchovávania. Hoci Komisár pre vyšetrovacie právomoci uvádza, že sa prijali opatrenia a zaviedli sa záruky, niektoré z nich sú naďalej vykonávané manuálne a vedú sa na individuálnom ľudskom základe, pričom podotýka, že je kľúčové, aby *„Bezpečnostná služba (MI5) naďalej udržiavala tieto nové postupy a vyčlenila dostatočné zdroje na ich účinné fungovanie. Ak Bezpečnostná služba (MI5) zaznamená nárast správania, ktoré nie je v súlade s predpismi,“*[116] Komisár pre vyšetrovacie právomoci očakáva, že ho na ne neodkladne upozorní. **EDPB preto vyzýva Európsku komisiu, aby v budúcnosti tieto aspekty pozorne sledovala.**

183. Pokiaľ ide o Vládne komunikačné ústredie, EDPB zároveň na základe správy Komisára pre vyšetrovacie právomoci chápe, že v súvislosti s operáciami vykonávanými na základe hromadných príkazov sa *„kvalita žiadostí o vnútorné schválenie líšila a pozorovali sme priestor na zlepšenie týkajúci sa spôsobu predkladaní takýchto žiadostí“*[117] a že v súvislosti s cieleným zasahovaním do zariadení boli vysvetlenia použitia všeobecných deskriptorov často príliš všeobecné a nepresné.[118] EDPB zároveň v súvislosti s hromadným zasahovaním do zariadení berie na vedomie, že Komisár pre vyšetrovacie právomoci odporúča, *„aby žiadosti konzistentne a výslovne zaznamenávali prepojenie medzi cieľom a zákonnými účelmi a spravodajskými požiadavkami“*[119] a že *„všetky žiadosti by mali pri posudzovaní proporcionality jasne zohľadniť možnosť vedľajšieho zásahu a príslušné zmiernenia“*[120], a to, že Komisár pre vyšetrovacie právomoci zdôrazňuje to, že napriek dosiahnutému pokroku *„stále existuje priestor na zlepšenie“*[121] a ďalšia pozornosť bude nevyhnutná aj v budúcnosti.

184. V súvislosti so systémom pre hromadné zachytávanie podľa zákona o regulácii vyšetrovacích právomocí z roku 2000 (ďalej len „RIPA z roku 2000“), ktorý bol medzitým nahradený ustanoveniami zákona o vyšetrovacích právomociach z roku 2016, EDPB pripomína, že nedostatočná miera dohľadu nad výberom internetových nositeľov na zachytávanie a filtrovanie, aj nad filtrovaním, vyhľadávaním a výberom zachytávanej komunikácie na preskúmanie, predstavovala jeden z kľúčových aspektov, o ktorých Európsky súd pre ľudské práva v rámci rozsudku vo veci *Big Brother Watch,* ktorý je v súčasnosti postúpený na veľkú komoru, rozhodol, že nie sú v súlade s článkom 8 EDĽP so zreteľom na predchádzajúce právne predpisy týkajúce sa vyšetrovacích právomocí orgánov Spojeného kráľovstva v kontexte národnej bezpečnosti. **EDPB vyzýva Európsku komisiu, aby overila súčasný stav postupov, zohľadnila tieto prvky a uviedla ich v rozhodnutí o primeranosti, ak ho má Európska komisia prijať.**

185. V tejto veci Európsky súd pre ľudské práva: „*nebol presvedčený, že záruky upravujúce výber nositeľov na zachytávanie a výber zachyteného materiálu na preskúmanie sú dostatočné spoľahlivé na to, aby poskytovali primerané záruky pred ich zneužitím. Najväčšie obavy však vzbudzuje absencia spoľahlivého nezávislého dohľadu nad selektormi a kritériami vyhľadávania, ktoré sa používajú na filtrovanie zachytenej komunikácie.“*[122] Ako zdôraznil Komisár pre vyšetrovacie právomoci, *„tento*

[116] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 8.52.
[117] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.2.
[118] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, body 10.16 a 10.17.
[119] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.23.
[120] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.23.
[121] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.23.
[122] Pozri rozsudok ESĽP, Big Brother Watch, bod 347.

záver odráža podobné odporúčanie v správe Výboru pre spravodajstvo a bezpečnosť ‚Súkromie a bezpečnosť: moderný a transparentný právny rámec' z marca 2015."[123] **EDPB víta skutočnosť, že Komisár pre vyšetrovacie právomoci následne v roku 2019 vykonal preskúmanie svojho prístupu ku kontrole hromadného zachytávania, *„ktoré obsahuje dôkladné preskúmanie technicky komplexných spôsobov vykonávania hromadného zachytávania v praxi"*[124] a v ktorom sa zaviazal zahrnúť *„podrobné preskúmanie selektorov a kritérií vyhľadávania, na ktoré poukázal Európsky súd pre ľudské práva"*[125] v kontrolách hromadného zachytávania od roku 2020. Vzhľadom na dôležitosť tohto aspektu je EDPB znepokojený tým, že Komisár pre vyšetrovacie právomoci doposiaľ nevykonal podrobné preskúmanie selektorov a kritérií vyhľadávania a Európsku komisiu vyzýva, aby pozorne sledovala vývoj v tejto súvislosti, najmä preto, že je potrebné objasniť konkrétny formát takého dohľadu.**[126]

4.3.2. Ďalšie používanie získaných informácií na účely národnej bezpečnosti a poskytovanie údajov do zahraničia

186. Pokiaľ ide o ďalšie používanie získaných informácií na účely národnej bezpečnosti, Európska komisia vo svojom posúdení odkazuje na § 87 ods. 1 zákona o ochrane údajov z roku 2018, v ktorom sa skutočne stanovuje, že *„takto získané osobné údaje sa nesmú spracúvať spôsobom nezlučiteľným s účelom, na ktorý boli získané."* EDPB však podotýka, že na toto ustanovenie sa môžu vzťahovať výnimky v záujme národnej bezpečnosti podľa § 110 zákona o ochrane údajov z roku 2018. EDPB okrem toho poznamenáva, že v právnych predpisoch, pokiaľ ide o cielené zachytávanie a preskúmavanie, cielené získavanie a uchovávanie údajov o komunikácii, cielené zasahovanie do zariadení alebo hromadné zachytávanie a hromadné zasahovanie do zariadení, sa stanovuje možnosť „poskytovania údajov do zahraničia".

4.3.2.1. Ďalšie používanie, poskytovanie údajov a uplatniteľný právny rámec v Spojenom kráľovstve

187. Európska komisia identifikovala časť 4 zákona o ochrane údajov z roku 2018, a najmä v nej obsiahnutý § 109, ako relevantné ustanovenia, ktorými sa stanovujú konkrétne požiadavky na ďalšie používanie získaných informácií, a najmä medzinárodný prenos osobných údajov spravodajskými službami do tretích krajín alebo medzinárodným organizáciám. EDPB však poznamenáva, že v § 110 zákona o ochrane údajov z roku 2018 sa stanovujú výnimky v záujme národnej bezpečnosti, v ktorých sa uvádza, že určité ustanovenia zákona o ochrane údajov z roku 2018 sa neuplatňujú, ak je výnimka z týchto ustanovení požadovaná na účely ochrany národnej bezpečnosti. Súčasťou dotknutých ustanovení, ktoré sa nemusia uplatňovať, je časť 4 kapitola 2 zákona o ochrane údajov z roku 2018 vo vzťahu k zásadám ochrany údajov vrátane obmedzenia účelu, ako aj časť 4 kapitola 3 zákona o ochrane údajov z roku 2018 vo vzťahu k právam dotknutých osôb. Ustanovenia § 109 zákona o ochrane údajov z roku 2018 v spojení s § 110 zákona o ochrane údajov z roku 2018 a podmienkami, za akých sa uplatňujú, môže viesť k prípadom, v ktorých medzinárodný prenos osobných údajov spravodajskými službami do tretích krajín prebieha bez toho, aby sa uplatňovali ustanovenia v súvislosti so zásadami ochrany údajov a s právami dotknutých osôb.

188. Ako uvádza Európska komisia, takéto výnimky sa musia posudzovať jednotlivo a môžu sa uplatniť len vtedy, ak by uplatňovanie konkrétneho ustanovenia malo negatívne dôsledky na národnú bezpečnosť. Cieľom vydávania osvedčení o záujme národnej bezpečnosti pre spravodajské služby

[123] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.28.
[124] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.28.
[125] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.28.
[126] Pozri výročnú správu Komisára pre vyšetrovacie právomoci z roku 2019, 15. december 2020, bod 10.28: „presný formát tejto kontroly sa ešte musí schváliť."

Spojené kráľovstva je v skutočnosti potvrdiť, že výnimka sa požaduje vo vzťahu k určeným osobným údajom, ktoré sa spracúvajú na účely ochrany národnej bezpečnosti. EDPB však poznamenáva, že ministerstvo vnútra Spojeného kráľovstva vo svojom usmernení k osvedčeniam o záujme národnej bezpečnosti podľa zákona o ochrane údajov z roku 2018 objasňuje, že *„[j]e potrebné hneď na začiatku uviesť, že osvedčenia nie sú potrebné na uplatnenie výnimiek v záujme národnej bezpečnosti; v skutočnosti vo väčšine prípadov samotní prevádzkovatelia stanovia, či sa uplatňuje výnimka v záujme národnej bezpečnosti.“* [127] Okrem toho ministerstvo vnútra Spojeného kráľovstva v usmernení uvádza, že *„osvedčenia o záujme národnej bezpečnosti sa môžu uplatniť na osobné údaje, ktoré možno konkrétne identifikovať alebo sa môžu vzťahovať na širšiu kategóriu osobných údajov. Môžu byť preventívne, ako aj retrospektívne.“* [128] Výnimky v záujme národnej bezpečnosti sa preto môžu uplatňovať na medzinárodný prenos osobných údajov spravodajskými službami do tretích krajín bez osvedčenia o záujme národnej bezpečnosti.

189. EDPB okrem toho berie na vedomie, že napríklad v osvedčení o záujme národnej bezpečnosti DPA/S27/Security Service[129] sa uvádza, že do 24. júla 2024 spracúvané osobné údaje *„pre Bezpečnostnú službu, v jej mene, na jej požiadanie alebo s jej pomocou“* a tam, *„kde je takéto spracúvanie nevyhnutné na uľahčenie riadneho výkonu funkcií Bezpečnostnej služby uvedených v § 1 zákona o bezpečnostných službách z roku 1989,“* sa vynímajú z príslušných ustanovení kapitoly V všeobecného nariadenia o ochrane údajov v práve Spojeného kráľovstva týkajúcich sa prenosu osobných údajov do tretích krajín alebo medzinárodným organizáciám. Hoci iné verejne dostupné osvedčenia o záujme národnej bezpečnosti neposkytujú výnimku z ustanovení § 109 zákona o ochrane údajov z roku 2018, treba pripomenúť, že časť alebo úplné znenie osvedčenia o záujme národnej bezpečnosti sa môže zamietnuť, ak by jeho zverejnenie bolo v rozpore so záujmami národnej bezpečnosti, v rozpore s verejným záujmom alebo ak by mohlo ohroziť bezpečnosť akejkoľvek osoby.

190. Vo všeobecnosti EDPB v rámci posúdenia návrhu rozhodnutia v súvislosti s týmito ustanoveniami pozoruje, že záruky pre tieto poskytovania údajov zahŕňajú výlučne požiadavku, aby príjemca údajov dodržiaval požiadavky týkajúce sa bezpečnosti údajov, rozsahu poskytovania údajov obmedzeného na to, čo je nevyhnutné, uchovávania údajov a prístupu obmedzeného počtu osôb k údajom. **EDPB preto zdôrazňuje, že pokiaľ ide o poskytovanie údajov do zahraničia, uplatňovanie výnimky v záujme národnej bezpečnosti stanovené v právnych predpisoch Spojeného kráľovstva môže viesť k situáciám, v ktorých by neboli záruky, ktorými sa zabezpečujú zásady obmedzenia účelu, nevyhnutnosti a proporcionality, ako aj práva jednotlivcov, dohľad a prostriedky nápravy, v plnej miere stanovené alebo dodržiavané v tretej cieľovej krajine. EDPB preto odporúča Európskej komisii, aby ďalej preskúmala celkové záruky stanovené v právnych predpisoch Spojeného kráľovstva, pokiaľ ide o poskytovanie údajov do zahraničia, najmä so zreteľom na uplatňovanie výnimiek v záujme národnej bezpečnosti.**

4.3.2.2. Poskytovanie údajov do zahraničia a výmena spravodajských informácií v kontexte medzinárodnej spolupráce

191. EDPB takisto berie na vedomie, že Európska komisia ako súčasť svojho posúdenia primeranosti nezohľadnila platné medzinárodné dohody medzi Spojeným kráľovstvom a tretími krajinami alebo

[127] Pozri ministerstvo vnútra, zákon o ochrane údajov 2018, Usmernenie o osvedčeniach o záujme národnej bezpečnosti, august 2020, bod 3, s. 3.
[128] Pozri ministerstvo vnútra, zákon o ochrane údajov 2018, Usmernenie o osvedčeniach o záujme národnej bezpečnosti, august 2020, bod 5, s. 4.
[129] Pozri DPA/S27/Security Service, § 27 zákona o ochrane údajov z roku 2018, osvedčenie ministra, 24. júla 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

medzinárodnými organizáciami, v ktorých sa môžu stanovovať osobitné ustanovenia týkajúce sa medzinárodného prenosu osobných údajov spravodajskými službami do tretích krajín.

192. EDPB zároveň zdôrazňuje, že posúdenie Európskej komisie sa opiera najmä o posúdenie časti 4 zákona o ochrane údajov z roku 2018, a vyjadruje obavy nad tým, že ustanovenia zákona o vyšetrovacích právomociach z roku 2016 sú zamerané na „žiadosti" na výmenu spravodajských informácií so zahraničnými partnermi, ale neriešia ďalšie formy výmeny spravodajských informácií. EDPB v tejto súvislosti poznamenáva, že v návrhu rozhodnutia Európskej komisie sa neuvádza ani neposudzuje prepojenie medzi právnym rámcom Spojeného kráľovstva a „Dohodou o komunikácii a spravodajstve medzi Spojeným kráľovstvom a USA". V nedávnom stanovisku pri príležitosti 75. výročia tejto dohody Národná bezpečnostná agentúra USA (ďalej len „NSA") uviedla, že toto partnerstvo umožňuje *„čo najväčšiu výmenu informácií medzi dvoma agentúrami pri minimálnych obmedzeniach„* a že *„sa týmto prelomovým dokumentom vytvorili politiky a postupy pre pracovníkov spravodajských služieb Spojeného kráľovstva a USA na výmenu komunikácie, preklad, analýzu a dekódovanie informácií."*[130] Táto dohoda zároveň tvorí základ ďalších spravodajských partnerstiev s Austráliou, Kanadou a Novým Zélandom.

193. Tajná povaha tejto dohody a jej osobitné ustanovenia predstavujú závažnú výzvu v súvislosti s jasnosťou a predvídateľnosťou právnych predpisov týkajúcich sa ďalšieho používania a poskytovania údajov do zahraničia, ktoré orgány Spojeného kráľovstva získali na účely národnej bezpečnosti. EDPB v tejto súvislosti pripomína, že pokiaľ ide o úroveň ochrany zaručenej v rámci EÚ, Súdny dvor EÚ zdôraznil, že v právnych predpisoch týkajúcich sa zásahu do základného práva na ochranu osobných údajov sa musia *„stanoviť jasné a presné pravidlá, ktoré budú upravovať rozsah a uplatnenie opatrenia a ukladať minimálne požiadavky tak, aby osoby, ktorých údaje boli prenesené, mali dostatočné záruky umožňujúce im účinne chrániť ich osobné údaje pred rizikami zneužitia, ako aj pred akýmkoľvek nezákonným prístupom a akýmkoľvek nezákonným použitím týchto údajov. Nevyhnutnosť disponovať takými zárukami je o to dôležitejšia v prípade, keď sú osobné údaje spracovávané automaticky a keď existuje značné riziko nezákonného prístupu k týmto údajom."*[131] EDPB sa preto domnieva, že Európska komisia by mala zvážiť vplyv dohody o komunikácii a spravodajstve medzi Spojeným kráľovstvom a USA ako súčasť jej posúdenia primeranosti.

194. Európsky súd pre ľudské práva v prvej časti svojho rozsudku z 13. septembra 2018 vo veci Big Brother Watch posúdil systém na výmenu spravodajských informácií, a najmä dohodu UK-US CI. Konkrétne Európsky súd pre ľudské práva uvádza, že *„[z]ákonný rámec, ktorým sa spravodajským službám Spojeného kráľovstva dovoľuje požiadať o zachytený materiál od zahraničných spravodajských služieb, nie je súčasťou zákona o regulácii vyšetrovacích právomocí. Dohoda medzi Spojeným kráľovstvo a Spojenými štátmi o komunikačnom spravodajstve z 5. marca 1946 umožňuje výmenu materiálu medzi Spojenými štátmi a Spojeným kráľovstvom"*[132] a domnieva sa, že existuje *„základ v zákone pre žiadosti o spravodajské informácie od zahraničných spravodajských služieb a že tento zákon je dostatočne prístupný."*[133] Napriek tomu, že Európsky súd pre ľudské práva dospel k záveru, že v súvislosti so systémami výmeny spravodajských informácií nedošlo k porušeniu článku 8[134] EDĽP, EDPB poznamenáva, že tento rozsudok bol postúpený veľkej komore, ktorej rozhodnutie je stále

[130] Pozri tlačovú správu NSA, Vládne komunikačné ústredie a NSA oslavujú 75 rokov partnerstva, 5. februára 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

[131] Pozri vec Schrems I, bod 91.

[132] Pozri rozsudok ESĽP, Big Brother Watch, bod 425.

[133] Pozri rozsudok ESĽP, Big Brother Watch, bod 427.

[134] Pozri rozsudok ESĽP, Big Brother Watch, bod 448.

otvorené. EDPB zároveň poznamenáva, že v čiastočne súhlasnom a čiastočne nesúhlasnom názore sudcu Koskela, ku ktorému sa pridal sudca Turković[135], dospel k záveru, že dochádza k porušeniu článku 8 EDĽP v súvislosti so systémom výmeny spravodajských informácií, pričom uvádza, že *„[j]e jednoduché sa stotožniť so zásadou, že by sa žiadnym systémom, ktorými sa získavajú spravodajské informácie z komunikácie, ktorá bola zachytená prostredníctvom zahraničných spravodajských služieb, či už na základe žiadostí o vykonanie takého zachytávania alebo poskytnutie jeho výsledkov, nemalo umožniť obchádzanie záruk zavedených pre každé sledovanie vnútroštátnymi orgánmi (pozri body 216, 423 a 447). Akýkoľvek iný prístup by bol vskutku neprijateľný.“*

195. Ako sa zdôrazňuje vo viacerých správach médií a mimovládnych organizácií[136][137], posledná verejne sprístupnená verzia dohody o komunikácii a spravodajstve medzi Spojeným kráľovstvom a USA pochádza z roku 1956, odkedy došlo k podstatným zmenám v oblasti komunikačných technológií a povahy signálového spravodajstva. V správach médií sa napríklad odhalilo, že údaje prechádzajúce podmorským káblovým vedením na území Spojeného kráľovstva sú zachytávané Vládnym komunikačným ústredím a sprístupňujú sa NSA.[138]

196. Z hľadiska EDPB predstavuje kľúčovú otázku v súvislosti s výmenou spravodajských informácií to, či sú § 109 zákona o ochrane údajov z roku 2018 a ustanovenia zákona o vyšetrovacích právomociach z roku 2016 naďalej uplatniteľné v prípade, ak spravodajské služby Spojeného kráľovstva konajú v súlade s dohodou o komunikácii a spravodajstve medzi Spojeným kráľovstvom a USA. Ďalším kľúčovým prvkom, ktorý sa má posúdiť, je to, či ustanovenia alebo účinné uplatňovanie tejto dohody majú vplyv na úroveň ochrany osobných údajov v tranzite z EHP do Spojeného kráľovstva alebo umožňujú priame získavanie osobných údajov spravodajskými službami tretích krajín a prístup k nim.

197. Okrem vyjadrených výhrad, pokiaľ ide o „poskytovanie údajov do zahraničia“ podľa časti 4 zákona o ochrane údajov z roku 2018 a jej príslušnej výnimky v záujme národnej bezpečnosti, ako aj o žiadosti v rámci zákona o vyšetrovacích právomociach z roku 2016, **EDPB teda vyjadruje znepokojenie v súvislosti s ďalšími formami výmeny informácií a poskytovania údajov na základe ďalších nástrojov, najmä rôznych medzinárodných dohôd uzavretých Spojeným kráľovstvom s inými tretími krajinami, najmä ak tieto nástroje nie sú prístupné verejnosti, ako je to v prípade dohody o komunikácii a spravodajstve medzi Spojeným kráľovstvom a USA. Vplyv takejto dohody by mohol viesť k obchádzaniu zavedených záruk týkajúcich sa použitia osobných údajov a prístupu k nim na účely národnej bezpečnosti.**

198. EDPB súhlasí s názorom osobitného spravodajcu OSN Joea Cannataccihо, ktorý uviedol, že *„[v]ýmena spravodajských informácií nesmie vytvárať „zadné dvierka“ na získavanie alebo uľahčenie získavania spravodajských informácií pre iné osoby bez vnútroštátnych záruk, ani medzeru pre vlády s nižšou*

[135] Pozri rozsudok ESĽP, Big Brother Watch, čiastočne súhlasný a čiastočne nesúhlasný názor sudcu Koskela, ku ktorému sa pridal sudca Turković.

[136] Pozri BBC, Denník odhaľuje zrod tajného paktu medzi Spojeným kráľovstvom a USA, ktorý sa rozrástol do skupiny „Pätica očí (Five Eyes), 5. marca 2021, https://www.bbc.com/news/uk-56284453.

[137] Pozri Privacy International, Politický briefing – Dohody Spojeného kráľovstva o výmene spravodajských informácií, apríl 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20 %28UK%29 %20FINAL.pdf.

[138] Pozri The Guardian, Vládne komunikačné ústredie odpočúva optické káble na tajný prístup k svetovým komunikáciám, 21. júna 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

úrovňou ochrany osobných údajov (alebo ďalších práv) na získavanie spravodajských informácií od spravodajskej služby Spojeného kráľovstva, ktoré by mohlo viesť k porušovaniu ľudských práv."[139]

199. **EDPB sa okrem toho v širšom zmysle domnieva, že uzatvorenie dvojstranných alebo viacstranných dohôd s tretími krajinami na účely spolupráce v oblasti spravodajstva, čím sa poskytne právny základ na priame zachytávanie a získavanie osobných údajov alebo prenos osobných údajov do týchto krajín, môže takisto zásadne vplývať na podmienky ďalšieho používania získaných informácií, keďže takéto dohody môžu mať vplyv na posudzovaný právny rámec ochrany údajov Spojeného kráľovstva.**

4.3.3. Dohľad

200. EDPB v súvislosti s primeranou úrovňou ochrany údajov zdôrazňuje dôležitosť komplexného dohľadu nezávislými dozornými orgánmi. Cieľom záruky nezávislosti dozorných orgánov v zmysle článku 8 ods. 3 Charty EÚ je zaručiť účinné a spoľahlivé monitorovanie dodržiavania pravidiel o ochrane jednotlivcov týkajúcich sa spracúvania osobných údajov.

201. Funkcie dohľadu v prípadoch používania osobných údajov a prístupu k nim na účely národnej bezpečnosti vykonáva najmä Komisár pre vyšetrovacie právomoci a Komisári pre justíciu (ďalej len „Komisári pre justíciu").

202. **EDPB vo všeobecnosti uznáva zavedenie Komisárov pre justíciu zákonom o vyšetrovacích právomociach z roku 2016 ako zásadné zlepšenie.** V súlade s uvedenou žiadosťou sa Európska komisia vyzýva, aby podrobnejšie posúdila **nezávislosť Komisárov pre justíciu, konkrétne do akej miery je právne zaručená nezávislosť Komisára pre vyšetrovacie právomoci a Úradu komisára pre vyšetrovacie právomoci, keďže v zákone o vyšetrovacích právomociach z roku 2016 sa neuvádza.** Je to o to dôležitejšie, keďže Komisár pre vyšetrovacie právomoci rozhoduje o odvolaniach v prípade, ak bola žiadosť o **opatrenie** sledovania zamietnutá **Komisárom pre justíciu**.

203. Komisár pre vyšetrovacie právomoci vykonáva funkcie dohľadu *ex-ante,* ako aj *ex-post.* Pokiaľ ide o dohľad *ex-ante*, EDPB to chápe tak, že funkciou Komisárov pre justíciu je jednotlivé schvaľovanie rôznych opatrení sledovania vrátane cieleného zachytávania a hromadného získavania údajov o komunikácii. EDPB ďalej poznamenáva, že predchádzajúce schválenie opatrení v oblasti sledovania nemožno odvodiť z jurisprudencie Súdneho dvora EÚ ako úplne nevyhnutnú požiadavku proporcionality opatrení sledovania.[140]

204. EDPB však s cieľom posúdiť účinnosť tejto úrovne dohľadu vidí potrebu ďalej objasniť scenáre, v ktorých je možné zákonné zachytávanie bez predchádzajúceho schválenia zo strany Komisárov pre justíciu.

205. Európska komisia v návrhu rozhodnutia uvádza v poznámkach pod čiarou č. 201 a 266 „konkrétne obmedzené prípady", ktoré sa stanovujú § 44 a § 52 zákona o vyšetrovacích právomociach z roku 2016 v súvislosti s cieleným zachytávaním. EDPB poznamenáva, že v § 45 až 51 zákona o vyšetrovacích právomociach z roku 2016 sa uvádzajú výnimky, ktoré sa údajne nemajú pravidelne používať spravodajskými službami. Navyše, **EDPB to chápe** tak, že v **prípadoch uplatňovania výnimiek** (napr. poskytovatelia telekomunikačných a poštových služieb) sa má vykonať predchádzajúce schválenie

[139] Pozri Záverečnú správu z misie osobitného spravodajcu OSN pre právo na súkromie na záver jeho misie v Spojenom kráľovstve Veľkej Británie a Severného Írska, Londýn, 29. júna 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

[140] Zároveň poznamenáva, že Súdny dvor EÚ pri zrušení platnosti štítu na ochranu údajov vo veci Schrems II zohľadnil skutočnosť, že podľa právnych predpisov USA tzv. súd FISA *„neschvaľuje jednotlivé opatrenia sledovania; schvaľuje skôr programy dohľadu (napríklad PRISM, UPSTREAM) na základe ročných osvedčení."* (bod 179).

Komisárom pre justíciu vtedy, ak orgány presadzovania práva alebo spravodajské služby **žiadajú** o prístup k týmto údajov, a **vyzýva Európsku komisiu, aby vo svojom rozhodnutí potvrdila správnosť tohto tvrdenia.**

206. EDPB uznáva, že podľa § 44 ods. 2 zákona o vyšetrovacích právomocí z roku 2016 sa umožňuje zachytávanie komunikácie, ak jedna zo strán (odosielateľ alebo príjemca) na to dala súhlas a ak existuje povolenie podľa zákona o regulácii vyšetrovacích právomocí z roku 2000 alebo zákona (Škótska) o regulácii vyšetrovacích právomocí z roku 2000 (zákon Škótskeho parlamentu č. 11 z roku 2000), t. j. predchádzajúceho právneho stavu pred zriadením Komisárov pre justíciu. EDPB **vyzýva** Európsku komisiu, aby objasnila, či to znamená, že v prípadoch existencie jednostranného súhlasu sa postup predchádzajúceho schválenia neuplatňuje vôbec.

207. Pokiaľ ide o dohľad *ex-post,* je dôležité overiť, že nezávislý dohľad je zaručený bez medzier, najmä vtedy, ak sa nepredpokladá *ex-ante.*

208. EDPB poznamenáva, že *ex-post* preskúmanie Komisármi pre justíciu sa vykonáva v rámci § 48 až § 52 zákona o vyšetrovacích právomociach z roku 2016, a **vyzýva Európsku komisiu, aby objasnila, na základe akých požiadaviek a na koho podnet sa má takéto *ex-post* preskúmanie vykonať.**

209. Podľa § 229 ods. 4 zákona o vyšetrovacích právomociach z roku 2016 Komisár pre vyšetrovacie právomoci nemá preskúmavať výkon určitých funkcií. EDPB v tejto súvislosti vyzýva Európsku komisiu, aby objasnila ustanovenia § 229 ods. 4. písm. d) a e) zákona o vyšetrovacích právomociach z roku 2016 týkajúcich sa praktického vplyvu na právomoc Komisára pre vyšetrovacie právomoci na preskúmanie. **EDPB to chápe tak, že ICO je oprávneným orgánom dohľadu vtedy, ak sa uplatňujú výnimky z § 229 ods. 4 zákona o vyšetrovacích právomociach z roku 2016 a EDPB vyzýva Európsku komisiu, aby vo svojom rozhodnutí potvrdila správnosť tohto tvrdenia.**

210. **Zdá sa**, že **úloha Komisára** pre vyšetrovacie právomoci je pri výkone dohľadu *ex-post* **obmedzená** na vydávanie odporúčaní v prípadoch nedodržania predpisov a oznámení dotknutej osobe, ak ide o závažnú chybu a ak je vo verejnom záujme, aby osoba bola informovaná. **EDPB vyzýva Európsku komisiu, aby objasnila, ako Úrad komisára pre vyšetrovacie právomoci môže účinne zabezpečiť dodržiavanie právnych predpisov.**

211. **EDPB napokon chápe, že dotknutí jednotlivci nemajú možnosť obrátiť sa na Úrad komisára pre vyšetrovacie právomoci priamo, ale musia podať sťažnosť ICO, ktorý však má obmedzené právomoci v oblasti národnej bezpečnosti. EDPB preto vyzýva Európsku komisiu, aby ďalej objasnila, ako je v týchto prípadoch právne zabezpečené riešenie sťažností zo strany Úradu komisára pre vyšetrovacie právomoci.**

4.3.4. Náprava

212. Vzhľadom na rozsudky Súdneho dvora EÚ vo veciach Schrems I a Schrems II je jasné, že účinná súdna ochrana v zmysle článku 47 Charty EÚ má zásadný význam na predpoklad primeranosti práva tretej krajiny. Z rozsudkov zároveň vyplýva, že mimoriadna pozornosť sa musí v tejto súvislosti venovať účinnej súdnej ochrane v oblasti prístupu k osobných údajom v záujme národnej bezpečnosti.

213. **EDPB uznáva, že Spojené kráľovstvo zriadilo IPT. IPT má právomoc pojednávať o prípadoch týkajúcich sa použitia vyšetrovacích právomocí nielen orgánmi presadzovania práva, ale aj spravodajskými službami. EDPB to chápe tak, že IPT funguje ako riadny súd v zmysle článku 47 Charty EÚ. Pokiaľ ide o jeho právomoci, Európska komisia sa vyzýva, aby potvrdila, že IPT má všetky tieto právomoci uvedené v odôvodnení 262 návrhu rozhodnutia, a to bez ohľadu na právny základ, v rámci ktorého sa sťažnosť podáva.**

214. Tajné sledovanie spravodajskými službami často znamená, že predmet sledovania, dotknutá osoba, nie je a nebude si vedomá sledovania. EDPB v tejto súvislosti pri analýze právnych predpisov USA vo viacerých prípadoch vyjadril znepokojenie nad podmienkou „žaloby“ v prípadoch sledovania, ako sa vykladá v právnych predpisoch USA. EDPB v tejto súvislosti poznamenáva, že IPT požaduje iba kritérium „presvedčenia“, podľa ktorého sťažovateľ musí preukázať riziko, že bude predmetom opatrenia.

215. EDPB pri analýze IPT zároveň venuje osobitnú pozornosť skutočnosti, že fungovanie IPT bolo opakovane v súlade s EDĽP podľa výkladu Európskym súdom pre ľudské práva.