
# Stanovisko 14/2021 k návrhu prováděcího rozhodnutí Evropské Komise podle nařízení (EU) 2016/679 o odpovídající ochraně osobních údajů ve Spojeném království

**Přijato dne 13. dubna 2021**

# OBSAH

**Evropský sbor pro ochranu osobních údajů**

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

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

s ohledem na články 12 a 22 svého jednacího řádu,

**PŘIJAL TOTO STANOVISKO:**

# 1. SHRNUTÍ

1. Evropská komise podpořila návrh prováděcího rozhodnutí (dále jen „návrh rozhodnutí“) o odpovídající ochraně osobních údajů ve Spojeném království podle GDPR dne 19. února 2021[2]. Evropská komise následně zahájila postup pro jeho formální přijetí.

2. Téhož dne Evropská komise požádala Evropský sbor pro ochranu osobních údajů (EDPB)[3] o vyjádření stanoviska. Posouzení odpovídající úrovně ochrany údajů přiznané ve Spojeném království provedl EDPB na základě přezkumu samotného návrhu rozhodnutí, jakož i na základě analýzy dokumentace, kterou mu zpřístupnila Evropská komise.

3. EDPB se při posouzení návrhu rozhodnutí zaměřil nejen na obecná hlediska GDPR, ale i na přístup orgánů veřejné moci k osobním údajům předávaným z EHP pro účely prosazování práva a národní bezpečnosti, včetně právních opravných prostředků, které jsou fyzickým osobám v EHP dostupné. EDPB rovněž posoudil, zda byly záruky stanovené v právním rámci Spojeného království zavedeny a zda jsou účinné.

4. Jako hlavní odkaz pro tuto činnost použil EDPB svůj referenční rámec pro odpovídající ochranu podle GDPR[4], přijatý v únoru 2018, a doporučení EDPB 02/2020 týkající se evropských základních záruk pro sledovací opatření[5].

[1] Pokud se v tomto stanovisku hovoří o „členských státech“, rozumějí se tím „členské státy EHP“.
[2] Viz tisková zpráva Evropské komise, Ochrana údajů: Evropská komise zahajuje postup v souvislosti s tokem osobních údajů do Spojeného království, 19. února 2021, https://ec.europa.eu/commission/presscorner/detail/cs/ip_21_661.
[3] Tamtéž.
[4] Viz pracovní skupina zřízená podle článku 29, Referenční rámec pro odpovídající ochranu, přijatý dne 28. listopadu 2017, v posledním znění přijatém dne 6. února 2018, WP 254 rev.01 (schválený EDPB, viz https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (dále jen „*referenční rámec GDPR pro odpovídající ochranu*“).
[5] Viz doporučení EDPB 02/2020 týkající se evropských základních záruk pro sledovací opatření, přijaté dne 10. listopadu 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_cs.

## 1.1 Oblasti sbližování

5. Hlavním cílem EDPB je poskytnout Evropské komisi stanovisko k odpovídající úrovni ochrany údajů přiznané fyzickým osobám ve Spojeném království. Je důležité vzít na vědomí, že EDPB neočekává, že by právní rámec Spojeného království replikoval evropské právo v oblasti ochrany údajů.

6. EDPB ovšem připomíná, že aby právní předpisy třetí země mohly být považovány za předpisy zajišťující odpovídající úroveň ochrany, musí být podle požadavku článku 45 GDPR a judikatury Soudního dvora Evropské unie (SDEU) uvedeny do souladu s podstatou základních zásad zakotvených v GDPR. Rámec Spojeného království pro ochranu osobních údajů se z velké části zakládá na rámci EU pro ochranu údajů (zejména na GDPR a směrnici Evropského parlamentu a Rady (EU) 2016/680, dále jen „směrnice o prosazování práva EU“), což vychází ze skutečnosti, že Spojené království bylo až do 31. ledna 2020 členským státem EU. Zákon Spojeného království o ochraně údajů z roku 2018, který vstoupil v platnost dne 23. května 2018 a zrušil zákon Spojeného království o ochraně údajů z roku 1998, navíc dále stanoví uplatňování GDPR v právních předpisech Spojeného království, vedle provádění směrnice o prosazování právních předpisů EU, jakož i udělování pravomocí a ukládání povinností vnitrostátnímu dozorovému úřadu pro ochranu údajů – britskému Úřadu komisaře pro informace (ICO). EDPB tedy uznává, že Spojené království ve většině případů odráží GDPR ve svém rámci pro ochranu osobních údajů.

7. **Je zřejmé, že při analýze právních předpisů a zvyklostí třetí země, která byla donedávna členským státem EU, EDPB shledal, že řada aspektů je v zásadě rovnocenná.**

8. EDPB uvádí, že v oblasti ochrany osobních údajů panuje mezi rámcem GDPR a právním rámcem Spojeného království značný soulad v případě některých klíčových ustanovení, jako jsou například pojmy (např. „osobní údaje“, „zpracování osobních údajů“, „správce údajů“), důvody pro zákonné a spravedlivé zpracování údajů pro legitimní účely, účelové omezení, kvalita a přiměřenost údajů, doba uchování údajů, bezpečnost a důvěrnost, transparentnost, zvláštní kategorie údajů, přímý marketing, automatizované rozhodování a profilování.

## 1.2 Výzvy

9. Spojené království bylo donedávna členským státem EU. Evropský sbor pro ochranu osobních údajů tudíž při analýze jeho právních předpisů a zvyklostí shledal, že řada aspektů je v zásadě rovnocenná. Zároveň se EDPB vzhledem ke své úloze v postupu zjišťování odpovídající úrovně ochrany údajů a také z důvodu časového omezení rozhodl zaměřit na takové aspekty, u nichž se domnívá, že vyžadují bližší pozornost a podrobnější prozkoumání.

10. Nadále však přetrvávají výzvy a EDPB se domnívá, že následující položky by měly být dále posouzeny, aby bylo zajištěno splnění v zásadě rovnocenné úrovně ochrany, kterou by měla Evropská komise ve Spojeném království podrobně sledovat.

### 1.2.1 Obecné informace

11. První, obecná výzva se týká sledování vývoje právního systému Spojeného království v oblasti ochrany údajů jako celku. Vláda Spojeného království skutečně naznačila svůj záměr vypracovat samostatné a nezávislé politiky v oblasti ochrany údajů s možným záměrem odchýlit se od právních předpisů EU o ochraně údajů. Tato politická prohlášení nebyla ještě v právním rámci Spojeného království uskutečněna. Nicméně taková případná budoucí odchylka **může představovat riziko pro zachování poskytované úrovně ochrany osobních údajů předávaných z EU. Proto se Evropská komise vyzývá k podrobnému sledování tohoto vývoje od okamžiku vstupu jejího rozhodnutí o**

**odpovídající ochraně v platnost a k přijetí nezbytných opatření, včetně změny rozhodnutí a/nebo případného pozastavení jeho použitelnosti.**

### 1.2.2 Obecné aspekty ochrany údajů

12. Za prvé, takzvaná „**imigrační výjimka**“ stanovená v **části 1** článku 4 **přílohy 2 zákona o ochraně údajů z roku 2018 je formulována „obecně“**. Platí totiž i v případě, kdy správce neshromažďuje osobní údaje pro účely imigrační kontroly, ale zpřístupní je jinému správci údajů, který tyto osobní údaje pro účely imigrační kontroly zpracovává.

13. EDPB vyzývá Evropskou komisi k ověření stavu řízení ve věci Open Rights Group & Anor, R (On the Application Of) v. Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), a jelikož tento rozsudek není konečným rozhodnutím (*res judicata*), také k ověření toho, zda bylo rozhodnutí potvrzeno, nebo je přezkoumáváno v rámci opravného prostředku, a aby veškeré aktualizace zohlednila a uvedla je ve svém rozhodnutí. **EDPB rovněž Evropskou komisi vyzývá, aby v rozhodnutí o odpovídající ochraně uvedla další informace o imigrační výjimce[6], zejména pokud jde o potřebnost a přiměřenost této obecné výjimky v právních předpisech Spojeného království, a to především s ohledem na širokou oblast osobní působnosti této výjimky.** EDPB zároveň vyzývá Evropskou komisi, aby dále prozkoumala, zda v právním rámci Spojeného království existují další záruky, nebo zda by mohly být stanoveny, například prostřednictvím právně závazných nástrojů, které by doplnily imigrační výjimku a posílily její předvídatelnost a záruky pro subjekty údajů, a rovněž umožnily lepší a rychlejší posouzení požadavků na potřebnost a přiměřenost.

14. Za druhé, ačkoli EDPB uznává, že Spojené království ve většině případů zkopírovalo kapitolu V GDPR do svého rámce pro ochranu osobních údajů, poukázal na některé aspekty právního rámce Spojeného království týkající se **dalšího předávání údajů**, jež by mohly znehodnotit úroveň ochrany osobních údajů předávaných z EHP.

15. Článek 44 GDPR[7] ostatně stanoví, že by předání a další předávání osobních údajů mělo probíhat, pouze pokud úroveň ochrany fyzických osob zaručená GDPR nebyla znehodnocena. **Nejenže tedy právní předpisy Spojeného království musí být „v zásadě rovnocenné“ právním předpisům EU, pokud jde o zpracování osobních údajů předávaných do Spojeného království podle budoucího rozhodnutí o odpovídající ochraně, ale také, že pravidla platná ve Spojeném království týkající se dalšího předávání těchto údajů do třetích zemí musí zajistit, aby v zásadě rovnocenná úroveň ochrany byla poskytována i nadále.**

16. Ačkoli EDPB uznává, že Spojené království má podle svého právního rámce působnost konstatovat, že území poskytují odpovídající úroveň ochrany na základě rámce Spojeného království pro ochranu údajů, EDPB by rád zdůraznil, že tato území doposud nemusí požívat výhod platného rozhodnutí o

[6] Také v důsledku probíhajícího přezkumu použití imigrační výjimky, jak je uvedeno na straně 5 vládního dokumentu Spojeného království „Explanatory Framework for Adequacy Discussions“, oddíl E3, příloha 2 Omezení, 13. března 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] *„K jakémukoli předání osobních údajů, které jsou předmětem zpracování nebo které jsou určeny ke zpracování po předání do třetí země nebo mezinárodní organizaci, může dojít pouze tehdy, splní-li správce a zpracovatel v závislosti na dalších ustanoveních tohoto nařízení podmínky stanovené v této kapitole, včetně podmínek pro další předávání osobních údajů z dané třetí země nebo mezinárodní organizace do jiné třetí země nebo jiné mezinárodní organizaci. Veškerá ustanovení této kapitoly se použijí s cílem zajistit, aby úroveň ochrany fyzických osob zaručená tímto nařízením nebyla znehodnocena.“*

odpovídající ochraně vydaného Evropskou komisí a zajišťovat úroveň ochrany „v zásadě rovnocennou“ úrovni ochrany zajištěné v EHP. To může vést k případnému ohrožení poskytované ochrany osobních údajů předávaných z EHP, zejména pokud se v budoucnu rámec Spojeného království pro ochranu osobních údajů odchýlí od *acquis* EU. Spojené království navíc již uznalo jako země zajišťující odpovídající úroveň ochrany takové třetí země, které požívají výhod ze zjištění Evropské komise ve věci odpovídající úrovně ochrany podle směrnice 95/46/ES[8], přičemž Evropská komise tato zjištění brzy přezkoumá, přičemž závěry tohoto přezkumu zatím nejsou známy.

17. **Ve výše uvedených případech by Komise měla plnit svou úlohu pozorovatele, a pokud nebude v zásadě rovnocenná úroveň ochrany osobních údajů předávaných z EHP zajištěna, měla by Evropská komise zvážit změnu rozhodnutí o odpovídající ochraně s cílem zavést zvláštní záruky pro údaje předávané z EHP a/nebo pozastavit použitelnost tohoto rozhodnutí.**

18. **Pokud jde o mezinárodní dohody uzavřené mezi Spojeným královstvím a třetími zeměmi**, Evropská komise se vyzývá, aby prověřila vzájemný vztah mezi rámcem Spojeného království pro ochranu údajů a jeho mezinárodními závazky, a to nad rámec dohody o přeshraničním přístupu k elektronickým důkazům pro účely boje proti závažné trestné činnosti, kterou uzavřely Spojené království a Spojené státy americké (dále jen „USA“)[9] (dále jen „dohoda podle zákona CLOUD Act mezi Spojeným královstvím a USA“), a to zejména proto, aby byla zajištěna nepřetržitá úroveň ochrany osobních údajů v případech, kdy jsou údaje předány z EU do Spojeného království na základě rozhodnutí Spojeného království o odpovídající ochraně a poté dále předány do jiných třetích zemí. Zároveň by měla nepřetržitě sledovat situaci a přijmout případná opatření, pokud by uzavření mezinárodních dohod mezi Spojeným královstvím a třetími zeměmi ohrozilo úroveň ochrany osobních údajů poskytovanou v EU.

19. Dále se Evropská komise vyzývá, aby sledovala, zda dohoda podle zákona CLOUD Act mezi Spojeným královstvím a USA zajišťuje příslušné další záruky vzhledem k citlivosti dotčených kategorií osobních údajů a podmínkám předávání elektronických důkazů přímo poskytovateli služeb, a nikoliv mezi orgány, a rovněž se vyzývá k posouzení, za jakých okolností lze záruky poskytnout, provedou-li se vhodné změny v zastřešující dohodě mezi EU a USA[10].

20. Kromě toho EDPB uvádí, že další předávání údajů může rovněž probíhat ze Spojeného království do jiné třetí země na základě **nástrojů pro předávání podle příslušných právních předpisů Spojeného království v oblasti ochrany osobních údajů[11]**. Po vzoru rozsudku ve věci Schrems II[12] EDPB vyzývá Evropskou komisi, aby v rozhodnutí o odpovídající ochraně poskytla ujištění, že potřebné záruky budou účinně zavedeny také s ohledem na právní předpisy přijímající třetí země.

21. Pokud jde o **ochranné prostředky podle článku 48 GDPR**, které v právních předpisech Spojeného království chybí, EDPB vyzývá Komisi, aby poskytla další ujištění a uvedla konkrétní odkazy na právní

[8] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, s. 31).
[9] Viz Dohoda mezi vládou Spojeného království Velké Británie a Severního Irska a vládou Spojených států amerických o přeshraničním přístupu k elektronickým důkazům pro účely boje proti závažné trestné činnosti, Washington D.C., USA, 3. října 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] Viz Dohoda mezi Spojenými státy americkými a Evropskou unií o ochraně osobních informací týkajících se prevence, vyšetřování, odhalování a stíhání trestných činů, prosinec 2016 (dále jen „zastřešující dohoda mezi EU a USA“), https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=LEGISSUM%3A3104_8.
[11] Viz články 46 a 47 GDPR Spojeného království.
[12] Viz Schrems II.

předpisy Spojeného království, které zajišťují, že úroveň ochrany údajů podle právního rámce Spojeného království bude v zásadě rovnocenná úrovni ochrany zajištěné v EHP.

22. Pokud jde o **procesní a donucovací mechanismy**, EDPB uvádí, že existence a účinné fungování nezávislého dozorového úřadu, existence systému zajišťujícího dobrou míru souladu s požadavky a systém zajišťující přístup k vhodným mechanismům nápravy, které fyzickým osobám v EHP poskytnou prostředky pro výkon jejich práv a domáhání se nápravy, aniž by se musely potýkat se složitými překážkami, které brání správní a soudní ochraně, jsou klíčovými prvky, jimiž se rámec pro ochranu údajů odpovídající evropskému rámci musí řídit.

23. EDPB uznává, že Spojené království ve většině případů zkopírovalo příslušná ustanovení GDPR do svého GDPR a zákona o ochraně údajů z roku 2018; přesto se Evropská komise vyzývá, aby nepřetržitě sledovala vývoj v právním rámci a postupech Spojeného království, jež by mohly mít na tyto oblasti škodlivý dopad.

### 1.2.3 Přístup orgánů veřejné moci k údajům předávaným do Spojeného království

24. EDPB poukazuje na podstatné změny v právním rámci Spojeného království, které se vztahují na bezpečnostní a zpravodajské agentury, zejména pokud jde o zachycování a získávání údajů v rámci komunikace. EDPB chápe, že tyto změny jsou mimo jiné reakcí na řízení zahájená před SDEU a Evropským soudem pro lidská práva (ESLP) a jejich nedávné rozsudky v této souvislosti.

25. EDPB zejména oceňuje, že Spojené království založilo Investigatory Powers Tribunal (tribunál pro kontrolu vyšetřovacích pravomoci, dále jen „IPT“). IPT má kompetenci rozhodovat ve věcech využití vyšetřovacích pravomocí nejen donucovacími orgány, ale i zpravodajskými službami. EDPB má tudíž za to, že IPT funguje jako řádný soud ve smyslu článku 47 Listiny základních práv Evropské unie (dále jen „Listina EU“).

26. Kromě toho EDPB vnímá ustavení „soudních komisařů“ v zákoně o vyšetřovacích pravomocích z roku 2016 (dále jen „IPA 2016“) jako výrazné zlepšení. Chápe, že důležitou úlohou soudních komisařů je v jednotlivých případech předem schvalovat různá kontrolní opatření, včetně cíleného zachycování a hromadného získávání údajů v rámci komunikace (tzv. postup dvojité pojistky).

27. Aby však mohla být posouzena účinnost této dodatečné úrovně dohledu, EDPB považuje za nutné dále objasnit situace, ve kterých je povoleno zákonné zachycování údajů bez souhlasu komisaře pro vyšetřovací pravomoci (dále jen „komisař IPC“) nebo bez souhlasu soudních komisařů, a vyzývá Evropskou komisi, aby dále posoudila a prokázala, že právní rámec Spojeného království poskytuje vhodné záruky i v případech, kdy neplatí postup dvojité pojistky, včetně záruk účinného dohledu *ex post* a dostupných opravných prostředků, čímž se zajistí úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany poskytnuté v EU.

28. EDPB navíc vyzývá Evropskou komisi, aby dále posoudila podmínky, za nichž lze použít zrychlený postup, a objasnila možnosti výkonu práv dotčených subjektů údajů a možné opravné prostředky, které mají k dispozici v souvislosti s vytěžováním počítačové sítě k získávání údajů, zejména v případě odchylky od postupu dvojité pojistky.

29. Kromě toho se EDPB domnívá, že je třeba dále vysvětlit a posoudit hromadné zachycování údajů, zejména výběr a použití selektorů, aby bylo objasněno, do jaké míry splňuje přístup k osobním údajům limit určený SDEU a jaké záruky jsou zavedeny na ochranu základních práv fyzických osob, jejichž údaje jsou v tomto ohledu zachycovány, včetně lhůt pro uchovávání údajů. Zvláště užitečné by bylo nezávislé posouzení, které by provedly příslušné orgány dohledu ve Spojeném království. EDPB rovněž zdůrazňuje, že situace je o to závažnější, že „přeshraniční komunikace“, na níž se

vztahují praktiky hromadného zachycování údajů, zdánlivě umožňuje, aby údaje z EU byly přímo zachycovány a hromadně shromažďovány Spojeným královstvím, a to včetně předávaných údajů mezi EU a Spojeným královstvím, na něž by se vztahoval návrh rozhodnutí. S ohledem na význam této skutečnosti EDPB vyzývá Evropskou komisi, aby podrobně sledovala vývoj v této oblasti.

30. V souvislosti s hromadným zachycováním údajů EDPB dále zdůrazňuje důsledné posuzování ze strany soudů ESLP a SDEU a připomíná obavy ohledně sekundárních údajů, které by z důvodu své citlivosti měly požívat výhod zvláštních záruk. EDPB proto vyzývá Evropskou komisi, aby důkladně posoudila, zda záruky stanovené v právních předpisech Spojeného království pro tuto kategorii osobních údajů zajišťují v zásadě rovnocennou úroveň ochrany jako v EHP.

31. V této souvislosti si je EDPB vědom, že se veřejná zpráva zpravodajského a bezpečnostního výboru o využívání hromadných pravomocí z roku 2016[13] zabývá postupy podle předchozího právního rámce, jež byl následně nahrazen zákonem IPA 2016. Domnívá se však, že je nutné provést další nezávislé posouzení a dohlížet nad používáním automatizovaných nástrojů pro zpracování ze strany příslušných orgánů dohledu ve Spojeném království, a vyzývá Evropskou komisi, aby dále tuto oblast posoudila, a to včetně záruk, které by v této souvislosti byly poskytovány, nebo mohly být poskytovány, subjektům údajů EHP.

32. EDPB sdílí stanovisko komisaře IPC, který považuje za nutné provést další přezkum a sledování s cílem zajistit, aby záruky, které v praxi používají příslušné orgány v oblasti národních bezpečnostních a zpravodajských služeb proti nedodržování pravidel pro uplatňování příslušných právních předpisů, byly zachovány a nadále zlepšovány. EDPB rovněž oceňuje, že komisař IPC následně provedl přezkum svého přístupu k hromadnému zachycování údajů v roce 2019, „*který zahrnoval pečlivý přezkum technicky složitých způsobů, v rámci nichž je hromadné zachycování skutečně prováděno*“ a zavázal se od roku 2020 provádět při kontrolách hromadného zachycování údajů „*podrobné posuzování selektorů a vyhledávacích kritérií, na něž ve výše uvedené souvislosti poukázal ESLP*“. Vzhledem k významu tohoto aspektu se EDPB obává, že důkladné posouzení selektorů a vyhledávacích kritérií ještě nebylo komisařem IPC provedeno, a vyzývá Evropskou komisi, aby podrobně sledovala vývoj v této oblasti, zejména z toho důvodu, že konkrétní formát takového dohledu je stále nutné objasnit.

33. EDPB upozorňuje, že v případě zahraničního zveřejňování údajů může uplatnění výjimky z důvodu národní bezpečnosti v právních předpisech Spojeného království vést k chybějícím zárukám, které by zajistily dodržování zásad účelového omezení, nezbytnosti a proporcionality, nebo stanovily, že dostatečná práva fyzických osob, dohled a opravné prostředky budou poskytovány nebo dodržovány ve třetí zemi určení. EDPB proto doporučuje, aby Evropská komise dále prozkoumala celkové záruky stanovené v právním řádu Spojeného království v případě zahraničního zveřejňování údajů, zejména pokud jde o použití výjimek z důvodu národní bezpečnosti.

34. EDPB je rovněž znepokojen používáním jiných forem sdílení a zveřejňování informací pomocí jiných nástrojů, především různých mezinárodních dohod, které Spojené království uzavřelo s dalšími třetími zeměmi, a zejména pokud takové nástroje zůstávají veřejnosti nepřístupné, například dohoda mezi Spojeným královstvím a USA o zpravodajské komunikaci (UK-US Communication Intelligence Agreement). Účinky takové dohody by mohly vést k obcházení stanovených záruk v oblasti přístupu k osobním údajům a jejich používání pro účely národní bezpečnosti. EDPB se domnívá, že uzavírání dvoustranných a mnohostranných dohod se třetími zeměmi pro účely spolupráce zpravodajských

[13] Viz přezkum zprávy o hromadných pravomocích provedený nezávislou osobou pro kontrolu právních předpisů v oblasti terorismu, srpen 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

služeb, jež poskytne právní základ pro přímé zachycování a získávání osobních údajů nebo pro předávání osobních údajů do třetích zemí, může rovněž významně ovlivnit podmínky dalšího používání shromážděných informací, jelikož tyto dohody pravděpodobně budou mít dopad na posuzovaný právní rámec Spojeného království pro ochranu údajů.

### 1.3 Závěr

35. EDPB se domnívá, že posouzení odpovídající úrovně ochrany údajů ve Spojeném království je unikátní z důvodu předchozího postavení Spojeného království jakožto členského státu. Kromě toho by se také jednalo o první rozhodnutí o odpovídající ochraně údajů, které by obsahovalo ustanovení o skončení platnosti.

36. EDPB tedy poukazuje na mnoho oblastí, v nichž se rámce pro ochranu údajů EU i Spojeného království sbližují. Zároveň však po důkladné analýze návrhu rozhodnutí Evropské komise a právních předpisů Spojeného království v oblasti ochrany údajů EDPB shledal řadu výzev, které jsou v tomto stanovisku důkladně prozkoumány. V tomto ohledu EDPB upozorňuje na rozhodující roli Evropské komise při sledování veškerého vývoje ve Spojeném království.

37. Vzhledem k výše uvedenému EDPB doporučuje, aby se Evropská komise zaměřila na řešení výzev uvedených v tomto stanovisku. EDPB rovněž vyzývá Evropskou komisi, aby podrobně sledovala veškerý vývoj ve Spojeném království, jenž by mohl mít vliv na zásadní rovnocennost úrovně ochrany osobních údajů, a aby v případě potřeby přijala vhodná opatření.

## 2. ÚVOD

### 2.1 Rámec Spojeného království pro ochranu údajů

38. Rámec Spojeného království pro ochranu osobních údajů se z velké části zakládá na rámci EU pro ochranu údajů (zejména na GDPR a směrnici o prosazování práva EU), což vychází ze skutečnosti, že Spojené království bylo až do 31. ledna 2020 členským státem EU. Zákon Spojeného království o ochraně údajů z roku 2018, který vstoupil v platnost dne 23. května 2018 a zrušil zákon Spojeného království o ochraně údajů z roku 1998, navíc dále stanoví uplatňování GDPR v právních předpisech Spojeného království, vedle provádění směrnice o prosazování právních předpisů EU, jakož i udělování pravomocí a ukládání povinností vnitrostátnímu dozorovému úřadu pro ochranu údajů – britskému úřadu ICO.

39. Jak je uvedeno ve 12. bodě odůvodnění návrhu rozhodnutí Evropské komise, vláda Spojeného království schválila zákon o Evropské unii (o vystoupení z Evropské unie) z roku 2018, který obsahuje přímo použitelné právní předpisy EU do právních předpisů Spojeného království. Podle tohoto zákona mají ministři Spojeného království pravomoc zavést pomocí zákonných předpisů sekundární právní předpisy, aby po vystoupení Spojeného království z EU mohly být provedeny potřebné úpravy v zachovaných právních předpisech EU tak, aby odpovídaly domácímu kontextu.

40. Příslušný právní rámec platný ve Spojeném království po konci přechodného období[14] se tudíž skládá z těchto předpisů:

[14] Přechodné období je stanoveno do 31. prosince 2020 a po tomto datu již právní předpisy EU nebudou ve Spojeném království platné. Tzv. „překlenovací období“ je stanoveno nejpozději do 30. června 2021 a představuje dodatečné období, během něhož se přenos osobních údajů z EHP do Spojeného království nepovažuje za předání.

- obecné nařízení Spojeného království o ochraně osobních údajů (dále jen „GDPR Spojeného království“), začleněné do právních předpisů Spojeného království podle zákona o Evropské unii (o vystoupení z Evropské unie) z roku 2018, ve znění nařízení DPPEC z roku 2019 (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)),
- zákon o ochraně údajů z roku 2018 (dále jen „DPA 2018“) ve znění nařízení DPPEC z let 2019 a 2020 (Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)) a
- zákon IPA 2016,

(společně jako „rámec Spojeného království pro ochranu údajů“).

## 2.2 Oblast posouzení sborem EDPB

41. Návrh rozhodnutí Evropské komise je výsledkem posouzení rámce Spojeného království pro ochranu údajů, po němž následovaly diskuse s vládou Spojeného království. V souladu s čl. 70 odst. 1 písm. s) GDPR se od EDPB očekává vypracování nezávislého stanoviska ke zjištěním Evropské komise, určení případných nedostatků v rámci odpovídající úrovně ochrany a snaha o předložení návrhů k jejich řešení.

42. Jak je uvedeno v referenčním rámci GDPR pro odpovídající ochranu: „*informace poskytnuté Evropskou komisí [by] měly být úplné a umožňovat Evropské radě pro ochranu údajů provést vlastní posouzení ochrany údajů ve třetí zemi*“[15].

43. V tomto ohledu je třeba poznamenat, že EDPB obdržel pouze částečnou dokumentaci potřebnou pro včasný přezkum právního rámce Spojeného království. Většinu právních předpisů Spojeného království, na které se odkazuje v návrhu rozhodnutí, obdržel EDPB prostřednictvím odkazů uvedených v daném návrhu. Evropská komise nebyla schopna poskytnout EDPB písemná vysvětlení a závazky Spojeného království týkající se výměn mezi orgány Spojeného království a Evropskou komisí, které jsou pro tuto analýzu důležité[16].

44. S ohledem na výše uvedené a také z důvodu omezeného časového rámce (2 měsíce), který má EDPB na přijetí tohoto stanoviska, se EDPB rozhodl zaměřit na některé konkrétní body uvedené v návrhu rozhodnutí, provést jejich analýzu a poskytnout na ně svůj názor.

[15] Viz WP 254 rev.01, s. 3.

[16] S ohledem na: článek 48 GDPR (poznámka pod čarou č. 78 v návrhu rozhodnutí); posílené záruky a bezpečnostní opatření, která uplatňují správci při zpracování údajů v souvislosti s národní bezpečností (poznámka pod čarou č. 64 v návrhu rozhodnutí); požadavek, aby správce uvážil, zda je nutné dovolávat se výjimky v jednotlivých případech, přestože bylo vydáno národní bezpečnostní osvědčení (126. bod odůvodnění a poznámka pod čarou č. 172 v návrhu rozhodnutí); skutečnost, že se ochranné prostředky zastřešující dohody mezi EU a USA budou vztahovat na všechny osobní údaje vytvořené nebo uchovávané podle dohody podle zákona CLOUD Act mezi Spojeným královstvím a USA, bez ohledu na povahu či druh orgánu, který o ně požádal, a s ohledem na podrobnosti konkrétního provádění záruk na ochranu údajů, jež jsou stále předmětem jednání mezi Spojeným královstvím a USA; potvrzení, že orgány Spojeného království nechají vstoupit tuto dohodu v platnost, jakmile budou přesvědčeny, že její provádění splňuje právní povinnosti z ní vyplývající, včetně objasnění souladu údajů vyžádaných v rámci této dohody s normami v oblasti ochrany údajů (153. bod odůvodnění návrhu rozhodnutí); situace, při kterých jsou v rámci návrhu rozhodnutí údaje předávány z EU do Spojeného království, přičemž se vždy bude jednat o „spojení s britskými ostrovy“ a jakýkoliv zásah zařízení zpracovávajících takové údaje by tudíž musel podléhat povinnému požadavku na soudní příkaz uvedenému v čl. 13 odst. 1 zákonu IPA 2016 (206. bod odůvodnění návrhu rozhodnutí), a příklady provozních účelů (216. bod odůvodnění a poznámka pod čarou č. 369 návrhu rozhodnutí).

45. Je zřejmé, že při analýze právních předpisů a zvyklostí třetí země, která byla donedávna členským státem EU, EDPB shledal, že řada aspektů je v zásadě rovnocenná. Vzhledem ke své úloze v postupu zjišťování odpovídající úrovně ochrany údajů a k množství právních předpisů a postupů, které je třeba analyzovat, se EDPB rozhodl zaměřit na takové aspekty, u nichž se domnívá, že vyžadují podrobnější prozkoumání. Kromě toho se v souladu s judikaturou SDEU velmi významná část analýzy týká právního režimu přístupu k osobním údajům předávaným do Spojeného království pro účely národní bezpečnosti a praxe bezpečnostních složek ve Spojeném království. Je však třeba mít na vědomí, že národní bezpečnost je očividně oblastí právních předpisů a zvyklostí, kde právní předpisy členských států nejsou harmonizovány na úrovni EU, a tudíž se mohou lišit.

46. EDPB zohlednil příslušný evropský rámec pro ochranu údajů, včetně článků 7, 8 a 47 Listiny EU, tedy ochranu práva na soukromý a rodinný život, právo na ochranu osobních údajů a právo na účinnou právní ochranu a spravedlivý proces, a článku 8 Evropské úmluvy o lidských právech (EÚLP), tj. ochranu práva na soukromý a rodinný život. Kromě výše uvedeného vzal EDPB v úvahu požadavky nařízení GDPR a příslušnou judikaturu.

47. Cílem této analýzy je poskytnout Evropské komisi stanovisko k posouzení odpovídající úrovně ochrany údajů ve Spojeném království. Tento koncept „odpovídající úrovně ochrany“, který existoval již ve směrnici 95/46/ES, byl dále rozpracován SDEU. Je nutné připomenout normu stanovenou SDEU ve věci Schrems I, konkrétně zásadu, že „úroveň ochrany“ ve třetí zemi musí být „v zásadě rovnocenná“ úrovni zaručované v EU, i když se „*prostředky, které tato třetí země využívá v tomto směru k zajištění takovéto úrovně ochrany, mohou lišit od prostředků zavedených v rámci Unie*“[17]. Cílem tedy není kopírovat legislativu EU krok za krokem, nýbrž stanovit základní a klíčové požadavky této legislativy. Odpovídající ochrany lze dosáhnout kombinací práv subjektů údajů a povinností subjektů, které údaje zpracovávají nebo nad takovým zpracováním vykonávají kontrolu, a dohledu prováděného nezávislými orgány. Pravidla ochrany údajů jsou však účinná jen tehdy, jsou-li vymahatelná a uplatňovaná v praxi. Je tedy nutné přihlížet nejen k obsahu pravidel platných pro osobní údaje předávané do třetí země nebo mezinárodní organizaci, ale i k systému zavedenému pro zajištění účinnosti těchto pravidel. Efektivní donucovací mechanismy mají pro účinnost pravidel vztahujících se na ochranu údajů zásadní význam[18].

## 2.3 Obecné připomínky a obavy

### 2.3.1 Mezinárodní závazky, které Spojené království přijalo

48. Podle čl. 45 odst. 2 písm. c) GDPR a referenčního rámce GDPR pro odpovídající ochranu[19] musí vzít Evropská komise při posuzování odpovídající úrovně ochrany ve třetí zemi v úvahu mimo jiné mezinárodní závazky, které třetí země přijala, nebo jiné povinnosti vyplývající z účasti třetí země v mnohostranných a regionálních systémech, zejména v souvislosti s ochranou osobních údajů, jakož i provádění těchto povinností. Dále by mělo být zohledněno přistoupení dané třetí země k Úmluvě Rady Evropy ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat (dále jen „úmluva č. 108“)[20], včetně jejího dodatkového protokolu[21].

[17] Viz rozsudek SDEU ze dne 6. října 2015, Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, (dále jen „Schrems I“), body 73–74.
[18] Viz WP 254 rev.01, s. 2.
[19] Viz WP 254 rev.01, s. 2.
[20] Viz Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, úmluva č. 108, 28. ledna 1981.
[21] Viz dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat, o dozorčích orgánech a toku údajů přes hranice, otevřený k podpisu dne 8. listopadu 2001.

49. **V tomto ohledu EDPB oceňuje, že se Spojené království řídilo Evropskou úmluvou pro lidská práva a spadá do působnosti Evropského soudu pro lidská práva. Kromě toho se Spojené království rovněž řídilo úmluvou č. 108 a jejím dodatkovým protokolem, v roce 2018 podepsalo úmluvu č. 108+[22] a v současné době pracuje na její ratifikaci.**

### 2.3.2 Možná budoucí odchylka rámce Spojeného království pro ochranu údajů

50. Jak je uvedeno v 281. bodě odůvodnění návrhu rozhodnutí, Evropská komise musí vzít v úvahu, že s koncem přechodného období, stanoveného v dohodě o vystoupení[23], Spojené království stanoví, uplatní a bude vymáhat svůj vlastní režim pro ochranu údajů, a jakmile přestane platit ustanovení o překlenovacím období podle článku FINPROV.10A Dohody mezi EU a Spojeným královstvím o obchodu a spolupráci[24], může dojít k úpravám nebo změnám posuzovaného rámce pro ochranu údajů, jakož i k dalšímu příslušnému vývoji.

51. Evropská komise se tudíž rozhodla zahrnout do svého návrhu rozhodnutí ustanovení o skončení platnosti[25], které je stanoveno na dobu čtyř let po jeho vstupu v platnost.

52. Je důležité poznamenat, že pokud britští ministři a státní tajemník(-ice) po konci překlenovacího období využijí možnosti zavést sekundární právní předpisy, může v budoucnu dojít ke značnému odchýlení rámce Spojeného království pro ochranu údajů od rámce EU.

53. Vláda Spojeného království opravdu naznačila svůj záměr vypracovat samostatné a nezávislé politiky v oblasti ochrany údajů, které mohou vést k odchýlení od právních předpisů EU o ochraně údajů[26].

[22] Viz Protokol o změně Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat („úmluva č. 108+“), 18. května 2018.
[23] Viz Dohoda o vystoupení Spojeného království Velké Británie a Severního Irska z Evropské unie a Evropského společenství pro atomovou energii (Úř. věst. L 29, 31.1.2020, s. 7).
[24] Viz Dohoda o obchodu a spolupráci mezi Evropskou unií a Evropským společenstvím pro atomovou energii na jedné straně a Spojeným královstvím Velké Británie a Severního Irska na straně druhé (Úř. věst. L 444, 31.12.2020, s. 14).
[25] Viz článek 4 návrhu rozhodnutí. Viz také 282. bod odůvodnění návrhu rozhodnutí.
[26] Spojené království ve své národní strategii v oblasti údajů (naposledy aktualizováno dne 9. prosince 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) jako jedno ze svých poslání uvádí následující: „*Prosazování mezinárodního toku údajů. Tok informací přes hranice podněcuje činnosti světového obchodu, dodavatelských řetězců a obchodování, čímž posiluje růst po celém světě. Zároveň plní širší společenskou roli. Předávání osobních údajů zajišťuje vyplácení mezd a pomáhá lidem spojit se se svými nejbližšími ze vzdálených míst. Jak názorně prokázala koronavirová pandemie, sdílení údajů o zdravotním stavu může napomoci při důležitém vědeckém výzkumu onemocnění a zároveň dokáže sjednotit státy ve společné reakci na mimořádné události v oblasti celosvětového zdraví.* ***Po svém odchodu z Evropské unie hodlá Spojené království prosazovat výhody, které údaje mohou přinášet.*** *Budeme podporovat domácí osvědčené postupy a spolupracovat s mezinárodními partnery, abychom* ***zajistili, že údaje nebudou nevhodným způsobem omezovány vnitrostátními hranicemi a nejednotnými regulačními systémy*** *a budou moci být využívány v plném rozsahu*“ (zvýraznění doplněno).

Tento záměr znamená začlenění aspektů osobních údajů do obchodních dohod[27], tj. postup, který s sebou nese riziko snížení úrovně ochrany osobních údajů, kterou Spojené království poskytuje[28].

54. Nejenže po skončení přechodného období nebude Spojené království nadále vázáno judikaturou SDEU, ale zároveň již přijaté rozsudky Soudního dvora, které jsou považovány za zachovanou judikaturu v právním rámci Spojeného království, již nebudou muset být pro Spojené království závazné. Spojené království smí po skončení překlenovacího období upravit zachované právní předpisy EU, a pro jeho Nejvyšší soud tak nebude závazná žádná zachovaná judikatura EU[29].

55. **S ohledem na rizika, která souvisejí s případným odchýlením rámce Spojeného království pro ochranu údajů od *acquis* EU po skončení překlenovacího období, EDPB oceňuje rozhodnutí Evropské komise zavést do návrhu rozhodnutí ustanovení o skončení platnosti. EDPB by však chtěla zdůraznit důležitost úlohy pozorovatele, kterou má Evropská komise[30]. Evropská komise by měla sledovat veškerý příslušný vývoj ve Spojeném království, jež by mohl ovlivnit v zásadě rovnocennou úroveň ochrany osobních údajů předávaných podle rozhodnutí Spojeného království o odpovídající ochraně, a to průběžným a trvalým způsobem od jeho vstupu v platnost. Evropská komise by navíc měla na základě zjištěných okolností přijmout příslušná opatření pozastavením použitelnosti, změnou nebo zrušením rozhodnutí o odpovídající ochraně, pokud po jeho přijetí zjistí, že odpovídající úroveň ochrany ve Spojeném království není nadále zajišťována.**

56. Pokud jde o EDPB, ten vynaloží veškeré úsilí, aby informoval Evropskou komisi o všech příslušných opatřeních, která dozorové úřady členských států pro ochranu údajů přijmou, ať už v obchodním, nebo veřejném sektoru, zejména s ohledem na podané stížnosti subjektů údajů týkající se předávání osobních údajů z EHP do Spojeného království.

# 3. OBECNÉ ASPEKTY OCHRANY ÚDAJŮ

## 3.1 Obsahové zásady

57. Kapitola 3 referenčního rámce GDPR pro odpovídající ochranu je věnována „obsahovým zásadám". Systém třetí země musí tyto zásady obsahovat, aby jeho úroveň ochrany mohla být považována za v zásadě rovnocennou úrovni ochrany zajištěné v EU. EDPB uznává skutečnost, že Spojené království

[27] Tamtéž: „*Usnadňování přeshraničních toků údajů:* ***Budeme celosvětově usilovat o odstranění zbytečných překážek mezinárodních toků údajů. Při obchodních jednáních dohodneme ambiciózní ustanovení týkající se údajů*** *a využijeme svého nově nezávislého postavení ve Světové obchodní organizaci, abychom obrátili pravidla obchodování k lepšímu.* ***Odstraníme překážky mezinárodního předávání údajů*** *na podporu růstu a inovací včetně vybudování nové schopnosti Spojeného království, která přinese nové a inovativní mechanismy pro mezinárodní předávání údajů. Rovněž budeme spolupracovat s partnery ve skupině G20, abychom zajistili interoperabilitu vnitrostátních systémů údajů s cílem snížit napětí při předávání údajů mezi státy*" (zvýraznění doplněno).

[28] Viz usnesení Evropského parlamentu ze dne 12. prosince 2017 „*Směrem ke strategii v oblasti digitálního obchodu*" (2017/2065(INI)), oddíl V, ve kterém je zdůrazněno, že „*ochrana osobních údajů je v obchodních dohodách [EU] nezpochybnitelná*", k dispozici na adrese: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_CS.pdf. Viz také usnesení Evropského parlamentu ze dne 25. března 2021 o hodnoticí zprávě Komise o provádění obecného nařízení o ochraně osobních údajů dva roky od začátku jeho uplatňování, bod 28, v němž se uvádí: „*podporuje praxi Komise, pokud jde o řešení ochrany osobních údajů odděleně od obchodních dohod*", https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_CS.html.

[29] Viz čl. 6 odst. 3 až 6 zákona o vystoupení z EU z roku 2018.

[30] Viz čl. 45 odst. 4 GDPR.

nemá psanou ústavu, v rámci níž by byla základní práva stanovena jedinou listinou. Nicméně právo na respektování soukromého a rodinného života (a právo na ochranu údajů jako součást tohoto práva) a právo na spravedlivý proces[31] jsou obsaženy v zákoně o lidských právech z roku 1998, jehož konstituční hodnotu soudy Spojeného království uznávají. Zákon o lidských právech z roku 1998 v podstatě přejímá práva uvedená v EÚLP[32]. Zákon o lidských právech z roku 1998 navíc velmi důležitě uvádí, že jakákoliv činnost orgánů veřejné moci musí být v souladu s EÚLP[33].

58. EDPB podle očekávání uvádí, že kromě strukturálních a formálních rozdílů v právních předpisech EU a Spojeného království, je přístup Spojeného království k ochraně údajů podobný jako přístup EU, což vyplývá ze skutečnosti, že Spojené království bylo až do 31. ledna 2020 členským státem EU. Mnoho obsahových zásad je tudíž v souladu se zásadami GDPR a poskytuje úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany poskytnuté v EU. EDPB rozhodl, že nebude vypracovávat další analýzu těchto obsahových zásad, které jsou v souladu s právními předpisy EU, a je spokojen s analýzou, kterou provedla Evropská komise ve svém návrhu rozhodnutí. Příklady těchto obsahových zásad jsou například tyto: pojmy (např. „osobní údaje“, „zpracování osobních údajů“, „správce údajů“), důvody pro zákonné a spravedlivé zpracování údajů pro legitimní účely, účelové omezení, kvalita a přiměřenost údajů, doba uchovávání údajů, bezpečnost a důvěrnost, transparentnost, zvláštní kategorie údajů, přímý marketing, automatizované rozhodování a profilování. EDPB dále uvádí, že GDPR Spojeného království a zákon DPA 2018 zahrnují obsahové zásady, které jsou nad rámec požadavků referenčního rámce GDPR pro odpovídající ochranu, a vycházejí ze zásad GDPR, a tudíž pozdvihují úroveň ochrany poskytované ve Spojeném království. Tyto obsahové zásady se týkají například oznámení o porušení osobních údajů, pověřence pro ochranu osobních údajů, posouzení dopadu na ochranu údajů a záměrné a standardní ochrany osobních údajů.

59. Jak je ovšem uvedeno v úvodu, EDPB se hodlá v tomto stanovisku konkrétně zabývat body, které u něj vyvolávají obavy, a rád by požádal Evropskou komisi o vysvětlení.

### 3.1.1 Právo na přístup, opravu, výmaz a námitku

60. Takzvaná „imigrační výjimka“ stanovená v **části 1** článku 4 **přílohy 2 zákona DPA 2018** umožňuje správcům údajů zapojeným do „imigrační kontroly“ neuplatňovat některá práva subjektů údajů stanovená v zákoně DPA 2018, pokud by taková situace pravděpodobně „*poškodila zachování účinné imigrační kontroly*“ nebo „*vyšetřování nebo odhalování činností, jež by narušily zachování účinné imigrační kontroly*“.

61. Jak se uvádí v návrhu rozhodnutí Evropské komise[34] a ve stanovisku výboru LIBE Evropského parlamentu o uzavření Dohody o obchodu a spolupráci mezi Evropskou unií a Spojeným královstvím[35], tato výjimka je **„obecně“ formulována**. Vztahuje se na tato práva: právo na informace, právo na přístup, právo na výmaz, právo na omezení zpracování a právo vznést námitku.

[31] Viz články 6 a 8 EÚLP (příloha 1 zákona o lidských právech z roku 1998).
[32] Podrobnější informace viz 8. až 10. bod odůvodnění návrhu rozhodnutí.
[33] Viz článek 6 zákona o lidských právech z roku 1998.
[34] Viz 62. až 65. bod odůvodnění návrhu rozhodnutí.
[35] Více informací o **obecné formulaci** imigrační výjimky viz stanovisko Výboru pro občanské svobody, spravedlnost a vnitřní věci o uzavření Dohody o obchodu a spolupráci mezi Evropskou unií a Evropským společenstvím pro atomovou energii na jedné straně a Spojeným královstvím Velké Británie a Severního Irska na straně druhé a Dohody mezi Evropskou unií a Spojeným královstvím Velké Británie a Severního Irska o bezpečnostních postupech pro výměnu a ochranu utajovaných informací jménem Unie (2020/0382(NLE)), 5. února 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_CS.pdf, bod 10:

62. Dále je důležité připomenout, že tato výjimka platí také v případě, kdy správce neshromažďuje osobní údaje pro účely imigrační kontroly („správce č. 1“), ale zpřístupní je jinému správci údajů („správce č. 2“), který tyto osobní údaje zpracovává pro účely imigrační kontroly (např. ministerstvo vnitra Spojeného království)[36].

63. Ve věci Open Rights Group & Anor, R (On the Application Of) v. Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (3. října 2019), žalobci napadli zákonnost imigrační výjimky z důvodu, že byla v rozporu s článkem 23 GDPR a nebyla slučitelná s právy zaručenými články 7 a 8 Listiny EU týkajících se soukromí a ochrany osobních údajů. Vrchní soud Anglie a Walesu (dále jen „Vrchní soud“) zvažoval, zda je imigrační výjimka stanovená v části 1 článku 4 přílohy 2 zákona DPA 2018 zákonná, a rozhodl ve prospěch její zákonnosti.

64. Vrchní soud došel zejména k závěru, že:

- *„[…] imigrační výjimka je očividně věcí ‚důležitého veřejného zájmu‘ a sleduje legitimní cíl […]“*, bod 30,
- *„imigrační výjimka splňuje požadavky na opatření, které je ‚v souladu se zákonem‘ […]“,* bod 38,
- *„O imigrační výjimku se lze opřít, pouze pokud by soulad s uvedenými ustanoveními GDPR‘ **pravděpodobně poškodil** zachování účinné imigrační kontroly či vyšetřování nebo odhalování činností, které by narušily zachování účinné imigrační kontroly. Výraz ‚pravděpodobně poškodil‘ byl v rámci zákona DPA 1998 (který předcházel zákonu DPA 2018) vykládán jako ‚velmi významné a závažné poškození konkrétního veřejného zájmu‘. Míra rizika musí být taková, aby stačilo ‚pouhé podezření‘ na poškození zájmů, i kdyby riziko bylo mnohem méně pravděpodobné než nepravděpodobné […].“*, bod 39 (zvýraznění doplněno).

---

*„připomíná v tomto ohledu usnesení Parlamentu z února a června 2020 a zdůrazňuje **obecnou a širokou výjimku** pro zpracovávání osobních údajů pro imigrační účely v případě zákona Spojeného království na ochranu údajů*“, a bod 11: „*domnívá se, že **obecnou a širokou výjimku** pro zpracovávání osobních údajů pro imigrační účely ze zákona Spojeného království na ochranu údajů […] bude nutné před tím, než bude moci být vydáno platné rozhodnutí ve věci přiměřenosti, změnit;*“ (zvýraznění doplněno).

[36] Viz příklad uvedený v „Guide to the General Data Protection Regulation (GDPR)“ (Pokyny k obecnému nařízení o ochraně osobních údajů (GDPR)) úřadu ICO, 1. leden 2021, s. 307 (zvýraznění doplněno): *„Soukromá organizace (správce č. 1) upozorní ministerstvo vnitra (správce č. 2) na zaměstnance, u nějž se domnívá, že předložil jako důkaz své totožnosti a kvalifikace pro získání pracovního místa falešnou dokumentaci. Zaměstnavatel poskytne ministerstvu vnitra příslušné informace. Právo osoby na informace o tom, že její osobní údaje byly předány ministerstvu vnitra, je omezené, jelikož by uplatnění takového práva pravděpodobně narušilo vyšetřování.*
***Zaměstnavatel tudíž nemá žádnou povinnost informovat osobu o tom, že její údaje byly předány ministerstvu vnitra** a **ministerstvo vnitra** zase nemá povinnost poskytnout osobě oznámení o ochraně osobních údajů, které by ji informovalo o tom, že jsou její osobní údaje aktuálně zpracovávány. Výjimka platí stejnou měrou pro oba správce.*
*Zaměstnanec však požádá ministerstvo vnitra, které jeho osobní údaje vyšetřuje, o jejich kopii. **Ministerstvo vnitra se může opřít o výjimku**, aby zatajilo tu část osobních údajů, jejíž zveřejnění by pravděpodobně narušilo vyšetřování. Pokud by zaměstnanec vznesl podobnou žádost na **svého zaměstnavatele, může i ten** ve stejné míře **uplatnit tuto výjimku**.“*
Jinými slovy, jak je uvedeno na s. 300: *„Ve většině případů bude správcem uplatňujícím tuto výjimku ministerstvo vnitra, případně některá z jeho agentur a zhotovitelů. Je však důležité upozornit, že se uplatnění této výjimky nevztahuje pouze na ministerstvo vnitra. Může být důležitá i pro jiné správce, například zaměstnavatele, univerzity a policii, kteří s ministerstvem vnitra jednají v imigračních záležitostech.“*

65. Je třeba podotknout, že tento rozsudek není podle informací EDPB konečný a bylo proti němu podáno odvolání.

66. Jak je uvedeno v pokynech EDPB k omezením podle článku 23 GDPR („pokyny k článku 23 GDPR“)[37] *„[…] v rámci GDPR jsou omezení **stanovena v legislativním opatření**, týkají se **omezeného počtu práv subjektů údajů a/nebo povinností správců**, které jsou uvedeny v článku 23 GDPR, **respektují podstatu** základních práv a svobod, představují **nezbytné a přiměřené opatření** v demokratické společnosti a zajišťují jeden z důvodů uvedených v čl. 23 odst. 1 GDPR […]“*.[38]

67. EDPB rovněž připomíná, že 41. bod odůvodnění GDPR uvádí, že *„[o]dkazy v tomto nařízení na **právní základ či legislativní opatření** neznamenají nutně legislativní akt přijatý parlamentem, aniž jsou dotčeny požadavky vyplývající z ústavního řádu dotčeného členského státu. Tento právní základ či legislativní opatření by však měly být **jasné a přesné a jejich použití by mělo být předvídatelné pro osoby, na něž se vztahují**, jak to vyžaduje judikatura Soudního dvora Evropské unie […] a Evropského soudu pro lidská práva*“ (zvýraznění doplněno).

68. Ačkoli ESLP uvedl, že *„[d]ále, pokud jde o výrazy ‚v souladu se zákonem‘ a ‚stanoví zákon‘, které se objevují v článcích 8 až 11 Úmluvy, [EÚLP] podotýká, že výraz ‚zákon‘ byl vždy chápán ve svém ‚materiálním‘ a nikoliv ‚formálním‘ pojetí; zahrnuje jak ‚psané právo‘ obsahující stejně tak podzákonné předpisy, jako regulační akty přijaté profesní organizací, delegací zákonodárce v rámci nezávislé zákonodárné pravomoci, tak i ‚nepsané právo‘. „Zákon“ musí být chápán tak, že zahrnuje jak psaný text, **tak ‚právo vytvořené soudci‘**“*[39], pokyny k článku 23 GDPR připomínají, že *„[p]odle judikatury SDEU, jakékoliv **legislativní opatření** přijaté na základě čl. 23 odst. 1 GDPR musí především **splňovat zvláštní požadavky stanovené v čl. 23 odst. 2 GDPR**. Ustanovení čl. 23 odst. 2 [nařízení] GDPR stanoví, že legislativní opatření omezující práva subjektů údajů a povinnosti správců údajů obsahují případná **konkrétní ustanovení o několika kritériích uvedených níže**. Zpravidla by všechny požadavky uvedené níže **měly být zahrnuty v legislativním opatření**, které ukládá omezení podle článku 23 [nařízení] GDPR*.“[40]

---

[37] Viz pokyny EDPB 10/2020 k omezením podle článku 23 GDPR, verze 1.0, přijaté dne 15. prosince 2020, které jsou po skončení veřejných konzultací v současné době ve fázi zpracování, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_cs.

[38] Viz pokyny k článku 23 GDPR, bod 9, s. 5.

[39] Viz rozsudek ESLP ze dne 14. září 2010, Sanoma Uitgevers B.V. v. Nizozemí, EC:ECHR:2010:0914JUD003822403, bod 83 (zvýraznění doplněno).

[40] Viz pokyny k článku 23 GDPR, body 45 a 46, s. 11. Podle čl. 52 odst. 3 Listiny EU, *„[p]okud tato listina obsahuje práva odpovídající právům zaručeným Úmluvou o ochraně lidských práv a základních svobod, jsou smysl a rozsah těchto práv stejné jako ty, které jim přikládá uvedená úmluva. Toto ustanovení nebrání tomu, aby právo Unie poskytovalo širší ochranu*.“ Pokud jde o výraz „**stanoveno zákonem**“ v čl. 52 odst. 1 Listiny EU, měla by se kritéria vypracovaná ESLP používat, jak navrhuje několik stanovisek generálního advokáta SDEU, viz například stanovisko ve spojených věcech C-203/15 a C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, body 137–154, a ve věci C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, body 88–114. Proto lze odkázat mimo jiné na rozhodnutí ESLP ve věci Weber a Saravia v. Německo, bod 84: *„Soudní dvůr opakuje, že výraz ‚**v souladu se zákonem**‘ ve smyslu čl. 8 odst. 2 EÚLP znamená nejen, že opatření, které stanoví zásah, musí mít právní základ ve **vnitrostátním právu**; ale rovněž poukazuje na **kvalitu právních předpisů**, které musí být pro danou osobu přístupné, aby mohla být schopna předvídat následky, a zároveň musí být v souladu s právními pravidly*“ (zvýraznění doplněno).
Viz rovněž 41. bod odůvodnění GDPR: *„Tento [právní základ či] legislativní opatření by však měly být **jasné a přesné a jejich použití by mělo být předvídatelné pro osoby, na něž se vztahují**, jak to vyžaduje judikatura Soudního dvora Evropské unie (…) Evropského soudu pro lidská práva*“ (zvýraznění doplněno).

69. V tomto ohledu je možné konstatovat, že **imigrační výjimka jako taková neurčuje tyto prvky uvedené v čl. 23 odst. 2 GDPR**:

- „záruky proti zneužití údajů nebo protiprávnímu přístupu k nim či jejich protiprávnímu předání“, písmeno d),
- „specifikaci správců nebo kategorie správců“, písmeno e)[41],
- „rizika z hlediska práv a svobod subjektů údajů“, písmeno g),
- „právo subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na újmu účelu omezení“, písmeno h).

70. „Pokyny k obecnému nařízení o ochraně osobních údajů (GDPR)“ úřadu ICO[42], které obsahují kapitolu o „imigrační výjimce“, poskytují objasnění imigrační výjimky, ale **nemohou** pro ni samy o sobě stanovit závazná pravidla. Otázka „kvality právních předpisů“ je obzvláště důležitá, s ohledem na význam omezených pravidel a rozšíření výjimky[43].

---

[41] Viz výše uvedená věc Vrchního soudu, bod 54: *„Neshledávám nic protiprávního na tom, že je imigrační výjimka dostupná **všem správcům údajů**, kteří zpracovávají údaje pro stanovené účely. Jak žalovaní uvedli, bez ustanovení čl. 4 odst. 3 a 4 by imigrační výjimka byla prohlášena za neplatnou v případech, kdy jsou údaje získávány od třetích stran (například místní orgán nebo úřad HM Revenue and Customs) pro účely zachování účinné imigrační kontroly.“* (zvýraznění doplněno), čímž se potvrzuje **obecné** uplatnění omezení.

[42] „Pokyny k obecnému nařízení o ochraně osobních údajů (GDPR)“ úřadu ICO, 1. leden 2021, s. 299–307.

[43] Viz bod 57 výše uvedeného případu Vrchního soudu: *„Byl jsem informován panem Knightem, že komisař dokončuje zpracování pokynů k výjimce, které ovšem budou mít ‚zákonné‘ postavení pouze ve smyslu jejich vydání na základě pravomoci komisaře podle čl. 57 odst. 1 GDPR. Nebudou mít žádné právní postavení podle zákona DPA 2018.“*

Odůvodnění pro zavedení právně závazných pokynů, které podporuje úřad ICO, je uvedeno zejména v bodech 56 až 60 rozsudku:

*„56. Nakonec přistupuji k podání komisaře, které tvrdí, že bez doprovodných zákonných pokynů, které poskytnou záruky, pokud jde o význam a uplatnění imigrační výjimky, by výjimka nebyla přiměřeným prováděním čl. 23 odst. 1 GDPR. Pan Knight uvádí, že v případě doplnění takovými pokyny bude ustanovení přiměřené.*

*57. Byl jsem informován panem Knightem, že komisař dokončuje zpracování pokynů k výjimce, které ovšem budou mít ‚zákonné‘ postavení pouze ve smyslu jejich vydání na základě pravomoci komisaře podle čl. 57 odst. 1 GDPR. Nebudou mít žádné právní postavení podle zákona DPA 2018. Rozumím také, že ministerstvo vnitra vypracovalo návrh interních pokynů k imigrační výjimce pro zaměstnance (viz [22] výše). V praxi jsou pokyny vydané komisařem významné bez ohledu na jejich právní základ. Neexistuje ovšem žádná pravomoc komisaře, která by umožnila vydání „závazných“ pokynů stejného druhu, jaké měl na mysli Nejvyšší soud v případě Christian Institute (body 101 a 107). Zdá se, že primární právo by bylo vyžadováno v případě, že by bylo nutné, aby existovaly pokyny k imigrační výjimce stejného postavení jako kodexy zásad uvedené v článcích 121–124 zákona DPA 2018.*

*58. Ve své argumentaci ve prospěch zákonných pokynů pan Knight tvrdí, že situace, v rámci níž vznikne potřeba použít imigrační výjimku, nutně vyvolá obavy o potřebnosti a přiměřenosti použití a existence této výjimky. V právní souvislosti upozorňuje především na dvě věci. Za prvé, osobní údaje, na něž se imigrační výjimka vztahuje, budou již svou podstatou pravděpodobně obsahovat zvláštní kategorii údajů ve smyslu čl. 9 odst. 1 GDPR (tj. údaje ‚vypovídající o rasovém či etnickém původu‘). Takové údaje jsou v nařízení GPPR uvedeny, jelikož vyžadují vyšší úroveň ochrany (stanovisko 1/15 [2019] 3 C.M.L.R. 25 bod 141). Za druhé, základním předpokladem právních předpisů na ochranu údajů je zejména právo subjektu na přístup k osobním údajům, které je velmi důležité pro možnost uplatňování dalších práv, která jsou subjektům údajů poskytována (viz YS v. Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 bod 44).*

*59. Pan Knight uvádí čtyři body praktické povahy. Za prvé, když správci subjektům údajů nevysvětlí, že se spolehli na zákonnou výjimku, ani neuvedou podrobné důvody, nebude si subjekt údajů vědom, že tato výjimka byla*

71. Tím spíše „**zkouška předpojatosti**“ nestanoví požadavky, které by bránily zneužití nebo protiprávnímu přístupu či předávání údajů a které by mohly být zavedeny například ministerstvem vnitra.

72. S ohledem na výše uvedené EDPB podotýká, že je nezbytné další objasnění ohledně použití imigrační výjimky.

73. EDPB navíc poukazuje na chybějící právně závazný nástroj, který by objasnil, zda je imigrační výjimka v zásadě rovnocenná článku 23 GDPR a článkům 7 a 8 Listiny EU. Zároveň se EDPB domnívá, že nezbytnost a přiměřenost široké oblasti osobní působnosti imigrační výjimky musí Evropská komise lépe prokázat a podložit je důkazy.

74. **Závěrem EDPB vyzývá Evropskou komisi k ověření stavu řízení Open Rights Group & Anor, R (On the Application Of) v. Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), a jelikož v této věci nebylo pravomocně rozhodnuto (*res judicata*), k ověření, zda je rozhodnutí potvrzeno nebo přezkoumáváno v rámci opravného prostředku, a aby veškeré aktualizace zohlednila a uvedla je ve svém rozhodnutí o odpovídající ochraně. EDPB rovněž vyzývá Komisi, aby poskytla další informace o nezbytnosti a přiměřenosti imigrační výjimky, zejména s ohledem na širokou oblast osobní působnosti.**

75. **EDPB zároveň vyzývá Evropskou komisi, aby dále prozkoumala, zda v právním rámci Spojeného království existují další záruky, nebo zda by mohly být stanoveny, například prostřednictvím právně závazných nástrojů, které by doplnily imigrační výjimku a posílily její předvídatelnost a záruky pro subjekty údajů, a rovněž umožnily lepší a rychlejší posouzení požadavků na nezbytnost a přiměřenost.**

### 3.1.2 Omezení dalšího předávání

76. Článek 44 GDPR stanoví, že by předání a další předávání osobních údajů mělo probíhat, pouze pokud úroveň ochrany fyzických osob zaručená GDPR nebude znehodnocena. Osobní údaje předávané z EHP do Spojeného království na základě rozhodnutí o odpovídající ochraně by tedy měly těžit z úrovně ochrany v zásadě rovnocenné úrovni ochrany poskytnuté podle rámce EU pro ochranu údajů. **Znamená to tedy nejen, že právní předpisy Spojeného království musí být „v zásadě rovnocenné“ právním předpisům EU, pokud jde o zpracování osobních údajů předávaných do Spojeného království podle návrhu rozhodnutí, ale také, že pravidla platná ve Spojeném království týkající se dalšího předávání těchto údajů do třetích zemí musí zajistit, aby v zásadě rovnocenná úroveň ochrany byla poskytována i nadále.**

---

*použita, a nebude ji moci v důsledku toho zpochybnit. Za druhé, subjekty údajů budou odkázány na schopnost správců uplatňovat výjimku řádně, a pouze pokud to bude nezbytné. Ačkoli má každý subjekt údajů právo podat stížnost proti uplatnění výjimky ke komisaři nebo zahájit soudní řízení před soudy, je pravděpodobné, že si subjekt údajů nebude vědom svých práv a nebude mít finanční prostředky, aby učinil právní kroky v případě, kdy je nutné zajistit rychlé a přesné dodržování práv na ochranu údajů. Za třetí, je pravděpodobné, že jako přistěhovalec se bude subjekt údajů nacházet ve zranitelné pozici. Za čtvrté, nejedná se o teoretickou otázku s ohledem na důkazy žalovaných, pokud jde o uplatňování imigrační výjimky (viz [4] výše).*
*60. Pan Knight naznačuje, že existuje velká podobnost mezi touto výzvou týkající se imigrační výjimky a odůvodněním Nejvyššího soudu ve věci Christian Institute [2016] UKSC 51. Podotýká, že stejně jako ve věci Christian Institute, je imigrační výjimka obecná, používá neurčité výrazy, stanoví nízkou hranici, podléhá kontrolám, které nejsou z ustanovení zřejmé, a lze ji uplatnit na velmi širokou oblast situací a práv. Na rozdíl od věci Christian Institute neexistují v případě imigrační výjimky žádné veřejně dostupné pokyny a už vůbec ne zákonné postavení, což je nutné zohlednit.“*

77. Je tedy důležité, aby každé další předávání osobních údajů z EHP ze Spojeného království do jiné třetí země bylo řádně chráněno zárukami nebo aby bylo provedeno v souladu s pravidly o odchylkách[44], s cílem zajistit nepřetržitost ochrany poskytované právními předpisy EU. **Pokud by taková ochrana nemohla být zajištěna, nemělo by se další předávání osobních údajů z EHP uskutečnit.**

78. EDPB uznává, že Spojené království ve většině případů převzalo kapitolu V GDPR do svého GDPR (články 44 až 49) a zákona o ochraně údajů z roku 2018[45]. **EDPB však poukázal na některé aspekty právního rámce Spojeného království týkající se dalšího předávání údajů, jež by mohly znehodnotit úroveň ochrany osobních údajů předávaných z EHP.**

79. **První výzva**, kterou EDPB určil, se týká třetích zemí, mezinárodních organizací nebo území[46], která Spojené království na základě postupu uvedeného v zákoně DPA 2018 uzná jako vhodné příjemce. Další předávání osobních údajů z EHP se může uskutečnit ze Spojeného království do třetích zemí na základě možného budoucího nařízení Spojeného království o odpovídající ochraně[47].

80. Jak je uvedeno v 77. bodě odůvodnění návrhu rozhodnutí, britský(-á) státní tajemník(-ice) má po konzultaci s úřadem ICO[48] pravomoc uznat třetí zemi (nebo území nebo odvětví ve třetí zemi), mezinárodní organizaci nebo popis takové země, území, odvětví nebo organizace jako příjemce zajišťující odpovídající úroveň ochrany osobních údajů. Při posuzování odpovídající úrovně ochrany musí britský(-á) státní tajemník(-ice) zvážit stejné prvky, které musí posoudit Evropská komise podle čl. 45 odst. 2 písm. a) až c) GDPR, společně se 104. bodem odůvodnění GDPR a zachovanou judikaturou EU. To znamená, že příslušným kritériem pro posuzování odpovídající úrovně ochrany třetí země bude skutečnost, zda daná třetí země zajišťuje „v zásadě rovnocennou" úroveň ochrany, kterou zajišťuje Spojené království. Ačkoli EDPB uznává, že Spojené království má podle GDPR Spojeného království schopnost konstatovat, že území poskytují odpovídající úroveň ochrany na základě rámce Spojeného království pro ochranu údajů, EDPB by rád zdůraznil, že tato území možná nebudou moci požívat výhod platného rozhodnutí o odpovídající ochraně vydaného Evropskou komisí a zajišťovat úroveň ochrany „v zásadě rovnocennou" úrovni ochrany zajištěné v EU. To může vést k případnému ohrožení poskytované ochrany osobních údajů předávaných z EHP, zejména pokud se v budoucnu rámec Spojeného království pro ochranu osobních údajů odchýlí od *acquis* EU. Je třeba poznamenat, že v červenci 2020 Soudní dvůr EU v zásadním rozsudku Schrems II[49] prohlásil rozhodnutí o tzv. US Privacy Shield („štít na ochranu soukromí") za neplatné, neboť shledal, že právní rámec USA nemohl být považován za rámec poskytující v zásadě rovnocennou úroveň ochrany v porovnání s úrovní ochrany v EU. Nicméně již přijaté rozsudky SDEU, které jsou považovány za zachovanou judikaturu v právním rámci Spojeného království, již nebudou muset být pro Spojené království závazné, neboť Spojené království smí po skončení překlenovacího období upravit zachované právo Unie, a pro jeho Nejvyšší soud tak nebude závazná žádná zachovaná judikatura EU[50].

[44] Viz článek 49 GDPR Spojeného království.
[45] Viz články 17A, 17B, 17C a 18 zákona DPA 2018.
[46] Viz článek 17A zákona DPA 2018.
[47] Britská obdoba rozhodnutí o odpovídající ochraně podle GDPR.
[48] Viz čl. 182 odst. 2 zákona DPA 2018. Viz také Memorandum o porozumění týkající se úlohy úřadu ICO v rámci nových posouzení odpovídající ochrany, 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/.
[49] Viz Schrems II.
[50] Viz čl. 6 odst. 3 až 6 zákona o vystoupení z EU z roku 2018.

81. **EDPB vyzývá Evropskou komisi, aby podrobně sledovala postup posuzování odpovídající ochrany a kritéria posuzování orgánů Spojeného království, pokud jde o třetí země, a zejména takové třetí země, které EU neuznává jako odpovídající podle GDPR. Pokud Evropská komise zjistí, že ve třetí zemi, kterou Spojené království uznalo, není poskytována v zásadě rovnocenná úroveň ochrany, která je zaručena v EU, EDPB vyzývá Evropskou komisi, aby podnikla veškeré potřebné kroky, jako například změnu rozhodnutí Spojeného království o odpovídající ochraně tak, aby byly zavedeny zvláštní záruky pro osobní údaje pocházející z EHP a/nebo aby zvážila pozastavení použitelnosti rozhodnutí Spojeného království o odpovídající ochraně, pokud jsou osobní údaje předávané z EHP do Spojeného království předmětem dalšího předávání údajů do dané třetí země na základě nařízení Spojeného království o odpovídající ochraně.**

82. **Druhá výzva** se týká nadcházejícího přezkumu již existujících rozhodnutí o odpovídající ochraně oznámených Evropskou komisí v rámci směrnice 95/46/ES. Na základě uvedeného přezkumu bude Evropská komise s přihlédnutím k současným právním předpisům EU a nedávné judikatuře moci rozhodnout, že země, které dosud těžily z rozhodnutí o odpovídající ochraně, již nadále neposkytují v zásadě rovnocennou úroveň ochrany. Jak je ovšem uvedeno v článku 4 přílohy 21 zákona DPA 2018, Spojené království již tyto země uznalo jako země poskytující odpovídající úroveň ochrany. Ačkoli musí britský(-á) státní tajemník(-ice) provést přezkum těchto zjištění odpovídající úrovně ochrany ve lhůtě čtyř let, Evropská komise ve svém návrhu rozhodnutí uvádí, že tato zjištění odpovídající úrovně ochrany nepřestanou automaticky existovat, pokud by britský(-á) státní tajemník(-ice) požadovaný přezkum v uvedené čtyřleté lhůtě neprovedl(a)[51].

83. **EDPB vyzývá Evropskou komisi, aby po přezkumu již existujících rozhodnutí o odpovídající ochraně EU sledovala, zda země, kterou již nelze považovat za zemi poskytující odpovídající úroveň ochrany, je za takovou zemi stále považována Spojeným královstvím. Bude-li tomu tak, EDPB vyzývá Evropskou komisi, aby na základě 277. až 280. bodu odůvodnění přijala veškerá opatření k nápravě situace, například změnou rozhodnutí o odpovídající ochraně s cílem přidat další zvláštní požadavky pro osobní údaje pocházející z EHP a/nebo pozastavením použitelnosti rozhodnutí o odpovídající ochraně, pokud by osobní údaje předávané z EHP do Spojeného království byly předmětem dalšího předávání do dané třetí země. EDPB vyzývá Evropskou komisi, aby pokračovala v tomto sledování po celou dobu trvání rozhodnutí o odpovídající ochraně Spojeného království.**

84. **Třetí výzva** se týká dalšího předávání osobních údajů z EHP do nevyhovujících zemí na základě nástrojů pro předávání uvedených v článcích 46 a 47 GDPR Spojeného království. Ačkoli GDPR Spojeného království uvádí stejné nástroje pro předávání jako GDPR, EDPB zdůrazňuje, že je třeba zajistit, aby záruky uvedené v nařízeních poskytovaly účinnou ochranu ve třetí zemi, zejména s ohledem na rozsudek ve věci Schrems II.

85. Na základě rozhodnutí ve věci Schrems II, v němž SDEU připomíná, že poskytovaná ochrana osobních údajů v EU musí tyto údaje doprovázet, ať putují kamkoliv, již EDPB přijal původní doporučení týkající se doplňujících opatření[52] na případnou pomoc vývozcům, aby bylo zajištěno, že subjektům údajů bude přiznaná úroveň ochrany údajů v zásadě rovnocenná úrovni zajištěné v EU.

[51] Viz 82. bod odůvodnění návrhu rozhodnutí.

[52] Viz doporučení EDPB č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU, přijato dne 10. listopadu 2020, které se na základě veřejné konzultace v současné době dokončuje, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_cs.pdf.

86. Podle SDEU jsou vývozci údajů, případně ve spolupráci s dovozcem údajů ve třetí zemi, v jednotlivých případech odpovědní za ověření, zda právní předpisy a zvyklosti třetí země ovlivňují účinnost a vhodnost záruk uvedených v článku 46 GDPR o nástrojích pro předávání[53]. Pokud tomu tak je, měli by vývozci údajů přijmout doplňující opatření, aby napravili nedostatky v ochraně údajů a přizpůsobili ji úrovni požadované právními předpisy EU.

87. **EDPB vyzývá Evropskou komisi, aby v rámci zajištění nepřetržité ochrany uvedla v návrhu rozhodnutí ujištění, že pokud vývozci údajů ve Spojeném království použijí nástroje pro předávání uvedené v článcích 46 a 47 GDPR Spojeného království pro další předávání údajů EHP do dalších třetích zemí, posoudí tito vývozci údajů v jednotlivých případech rámec pro ochranu údajů třetí země, a bude-li to nezbytné, přijmou příslušná opatření, aby zajistili účinné dodržování záruk vybraného nástroje pro předávání s cílem zajistit úroveň ochrany v zásadě rovnocennou úrovni ochrany zajištěné v EU. EDPB zdůrazňuje, že bez těchto ujištění vzniká riziko, že úroveň ochrany v zásadě rovnocenná úrovni ochrany zajištěné v EU bude tímto dalším předáváním údajů ze Spojeného království oslabena.**

88. **Čtvrtá výzva** související s dalším předáváním údajů se týká mezinárodních dohod, které Spojené království uzavřelo, nebo v budoucnu uzavře, a možného přímého zpřístupnění těchto osobních údajů z EHP orgánům a smluvním stranám těchto třetích zemí. EDPB má silné obavy ohledně již uzavřené dohody podle zákona CLOUD Act mezi Spojeným královstvím a USA, přičemž Evropská komise tuto výzvu utvrzuje zdůrazněním, že „*možný vstup dohody v platnost může ovlivnit úroveň ochrany posuzované v tomto rozhodnutí*“[54]. Po vstupu této dohody v platnost budou na jejím základě osobní údaje předávané z EHP do Spojeného království podle návrhu rozhodnutí podléhat ustanovením této dohody, která stanoví podmínky pro přímé zpřístupnění údajů americkým orgánům, čímž bude ovlivněn rámec Spojeného království pro ochranu údajů, včetně ustanovení o dalším předávání údajů. Ustanovení dohody uzavřené s USA tudíž mohou výrazně ovlivnit úroveň ochrany údajů předávaných z EHP a poznamenat tak jejich ochranu. EDPB v této souvislosti uvádí, že Evropská komise ve 153. bodě odůvodnění svého návrhu rozhodnutí odkazuje na vysvětlení poskytnutá orgány Spojeného království, aniž by k nim uvedla citace nebo poskytla konkrétní písemné ujištění či závazky, ani neuvádí konkrétní právní ustanovení předpisů Spojeného království, která by těmto vysvětlením dala účinek.

89. EDPB již dříve tyto obavy vyjádřil v dopise, který zaslal Evropskému parlamentu dne 15. června 2020[55]. EDPB zdůraznil, že na základě „*acquis EU v oblasti ochrany údajů, zejména GDPR a směrnice o prosazování právních předpisů*“, má pochyby o tom, zda záruky v dohodě o zpřístupnění osobních údajů ve Spojeném království budou platit za určitých okolností, které ukládající povinnost zveřejnění pro USA, a zda jsou tyto záruky dostatečné s ohledem na normy EU tak, aby nebyla znehodnocena úroveň ochrany údajů poskytovaná v EU.

90. Ustanovení dohody podle zákona CLOUD Act mezi Spojeným královstvím a USA dále mohou výrazně ovlivnit hmotné a procesní podmínky, podle nichž lze osobní údaje, které jsou v držení správců nebo zpracovatelů ve Spojeném království, přímo zpřístupnit americkým orgánům, což má dopad na úroveň ochrany zajišťované v rámci právních předpisů Spojeného království. Aby mohla být poskytována úroveň ochrany v zásadě rovnocenná úrovni ochrany zajištěné v rámci práva Unie, je

[53] Viz Schrems II, bod 134.
[54] Viz 153. bod odůvodnění návrhu rozhodnutí.
[55] Viz odpověď EDPB členům Evropského parlamentu Sophii in’t Veld a Moritzi Körnerovi k dohodě podle amerického zákona CLOUD Act mezi Spojeným královstvím a USA, přijato dne 15. června 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

například *„zásadní, aby záruky v takové dohodě zahrnovaly předchozí povinné soudní povolení jako základní zajištění přístupu k metadatům a údajům o obsahu. Na základě předběžného posouzení nemohl EDPB s vědomím, že se tato dohoda týká použití vnitrostátního práva, toto jasné ustanovení ve smlouvě uzavřené mezi Spojeným královstvím a USA určit“*[56].

91. Ačkoli Evropská komise zdůrazňuje, že údaje získané v rámci této dohody budou mít prospěch z ochranných prostředků, které odpovídají zvláštním zárukám poskytovaným v tzv. „zastřešující dohodě mezi EU a USA“, EDPB má obavy, zda zavedení těchto záruk do dohody podle zákona CLOUD Act mezi Spojeným královstvím a USA na základě pouhé zmínky o obdobném použití bude dostatečné k tomu, aby tyto záruky splňovaly kritéria pro jasná, přesná a dostupná pravidla přístupu k osobním údajům, nebo zda tyto záruky budou dostatečně zakotveny tak, aby byly účinné a vymahatelné v rámci právních předpisů Spojeného království.

92. **EDPB tedy doporučuje, aby Evropská komise objasnila, jakým způsobem by tyto ochranné prostředky rovnocenné zvláštním zárukám v zastřešující dohodě mezi EU a USA měly být naplněny a na základě jakého právního nástroje by měly získat závazný charakter v právních předpisech Spojeného království.**

93. EDPB rovněž uvádí, že ustanovení dohody podle zákona CLOUD Act mezi Spojeným královstvím a USA ve spojení s článkem 3 amerického zákona CLOUD Act[57] vyvolávají otázky ohledně skutečného uplatňování záruk, které dohoda nabízí v případě přístupu amerických orgánů pro vymáhání práva k osobním údajům ve Spojeném království, jež jsou zpracovávány poskytovateli služeb elektronické komunikace nebo vzdálených výpočetních služeb (dále jen „poskytovatelé SEK“), kteří spadají do působnosti USA. Pokud by poskytovatel CSP nacházející se ve Spojeném království podléhal právním předpisům USA (např. jako dceřiná společnost americké společnosti), je nutné zjistit, zda by se americké orgány musely při získávání údajů spoléhat na dohodu podle zákona CLOUD Act mezi Spojeným královstvím a USA. Jelikož Evropská komise uvedla, že *„[z]vláštní pozornost bude věnována používání a úpravě ochranných prostředků v zastřešující dohodě mezi USA a Spojeným královstvím pro účely zvláštních druhů převodů“*, EDPB zdůrazňuje, že na základě jeho předběžného posouzení není zcela jasné, zda by se záruky zakotvené v dohodě podle zákona CLOUD Act mezi Spojeným královstvím a USA, a tudíž i záruky poskytované v zastřešující dohodě mezi EU a USA, vztahovaly na všechny případné žádosti o zpřístupnění údajů ve Spojeném království, které by americké orgány podaly podle amerického zákona CLOUD Act.

94. V budoucnu může Spojené království uzavřít další mezinárodní dohody nebo přijmout závazky se třetími zeměmi, které by se vztahovaly rovněž na osobní údaje předávané z EHP do Spojeného království podle návrhu rozhodnutí[58]. V závislosti na ustanoveních těchto dohod a na použití doložek o zvláštních zárukách mohou takové mezinárodní dohody zásahem do rámce Spojeného království pro ochranu údajů rovněž zásadně ovlivnit hmotné a procesní podmínky pro přístup orgánů třetí země k osobním údajům ve Spojeném království. To se týká zejména návrhu druhého dodatkového protokolu k Úmluvě Rady Evropy o počítačové kriminalitě (dále jen „Budapešťská úmluva“), který je v současné době projednáván stranami této úmluvy, jíž se účastní i několik zemí mimo EU. Druhý protokol ve skutečnosti obsahuje doložky, které mohou strany dle vlastního uvážení aktivovat, například udělení povolení či zamítnutí přístupu k údajům o obsahu. Ačkoli by všechny členské státy EU tyto doložky aktivovaly v souladu s pravidly EU pro ochranu údajů, v případě Spojeného království nebyla poskytnuta žádná záruka a Spojené království by se tak mohlo výrazně odlišovat od úrovně

[56] Viz výše uvedený dopis EDPB.
[57] Viz americký zákon CLOUD Act, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.
[58] Viz oddíl 2.3.3 výše.

ochrany, která by byla poskytována v EU. Dalším příkladem výše uvedené problematiky je Dohoda mezi Spojeným královstvím a Japonskem o komplexním hospodářském partnerství[59] (CEPA), tj. první obchodní dohoda Spojeného království uzavřená po brexitu, která vstoupila v platnost dne 1. ledna 2021[60] a která obsahuje ustanovení o osobních údajích[61]. EDPB dále uvádí, že Spojené království dne 1. února 2021 oficiálně oznámilo svou žádost o připojení ke Komplexní a progresivní dohodě o transpacifickém partnerství (CPTPP), jejíž součástí je dohoda o transpacifickém partnerství (dále jen TPP)[62].

95. EDPB uvádí, že kromě dohody podle zákona CLOUD Act mezi Spojeným královstvím a USA nejsou mezinárodní dohody uvedené výše v návrhu rozhodnutí zmíněny.

96. **EDPB vyzývá Evropskou komisi, aby:**

- **prověřila vzájemný vztah mezi rámcem Spojeného království pro ochranu údajů a jeho mezinárodními závazky mimo dohodu podle zákona CLOUD Act mezi Spojeným královstvím a USA, zejména, aby byla zajištěna nepřetržitá úroveň ochrany v případě dalšího předávání osobních údajů do jiných třetích zemí, které jsou předávány z EHP do Spojeného království na základě rozhodnutí Spojeného království o odpovídající ochraně, a aby nepřetržitě sledovala situaci a případně přijala opatření, pokud by uzavření dalších mezinárodních dohod mezi Spojeným královstvím a třetími zeměmi ohrozilo úroveň ochrany osobních údajů poskytovanou v EU,**
- **informovala EDPB o písemných závazcích orgánů Spojeného království a určila konkrétní ustanovení v právních předpisech Spojeného království v souvislosti s vysvětlením možného použití a provádění dohody podle zákona CLOUD Act mezi Spojeným královstvím a USA, jak je uvedeno ve 153. bodě odůvodnění návrhu rozhodnutí,**
- **sledovala v této souvislosti, zda kromě záruk, které by mohly být poskytnuty vhodným použitím a prováděním zastřešující dohody mezi EU a USA, zajišťuje dohoda podle zákona CLOUD Act mezi Spojeným královstvím a USA další vhodné záruky, které by zohlednily úroveň citlivosti dotčených kategorií údajů a speciální požadavky na předávání elektronických důkazů přímo poskytovateli SEK spíše než mezi orgány,**
- **posoudila dopad a potenciální rizika ustanovení o osobních údajích uvedená v mezinárodních dohodách, které Spojené království nedávno uzavřelo, například v dohodě CEPA.**

97. **Pátá výzva** se týká uplatňování výjimek při předávání osobních údajů do třetí země. Ačkoli jsou dostupné výjimky v GDPR Spojeného království stejné jako výjimky v GDPR, je důležité, že úřad ICO uplatňuje a bude i nadále uplatňovat výklad o použití těchto výjimek ve shodě s výkladem EDPB.

[59] Viz Dohoda mezi Spojeným královstvím a Japonskem o komplexním hospodářském partnerství [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Viz pokyny vlády Spojeného království pro obchodní dohody se zeměmi mimo EU, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Podle čl. 8.80 odst. 5 dohody CEPA se strany zavazují k podporování vývoje mechanismů, které podpoří slučitelnost mezi jejich různými právními přístupy k ochraně (osobních) údajů. Podle článku 8.84 se strany zavazují, že nezakážou ani neomezí přeshraniční předávání informací elektronickými prostředky, včetně osobních údajů, pokud tato činnost slouží k výkonu obchodní činnosti dané osoby ve smyslu dohody CEPA.

[62] Podle čl. 14.11 odst. 2 dohody TPP všechny strany umožní přeshraniční předávání informací elektronickými prostředky, včetně osobních údajů, pokud tato činnost slouží k výkonu obchodní činnosti dané osoby ve smyslu dohody.

Pokud tomu tak nebude nebo se Spojené království od tohoto výkladu v budoucnu odchýlí, vznikne riziko znehodnocení úrovně ochrany údajů předávaných do třetích zemí přes Spojené království.

98. **EDPB vyzývá Evropskou komisi, aby jako součást svého sledování konkrétně kontrolovala, zda výklad Spojeného království o použití výjimek zůstává shodný s výkladem EU. Pokud by se však Spojené království řídilo jiným výkladem o použití výjimek, jenž by znehodnotil úroveň ochrany, je důležité, aby Evropská komise přijala potřebné kroky změnou rozhodnutí o odpovídající ochraně, aby bylo zajištěno, že úroveň ochrany poskytovaná osobním údajům z EHP předávaným do Spojeného království nebude znehodnocena, pokud tyto údaje budou dále předávány ze Spojeného království do třetích zemí na základě různého výkladu o výjimkách.**

99. **Šestá**, konečná **výzva** v této části, se týká chybějících ochranných prostředků podle článku 48 GDPR v rámci Spojeného království pro ochranu údajů.

100. Evropská komise ve svém návrhu rozhodnutí skutečně objasňuje, že se v případě chybějících nařízení o odpovídající ochraně nebo vhodných záruk může předání uskutečnit pouze na základě výjimek stanovených v článku 49 GDPR Spojeného království, „*vyjma článku 48 nařízení (EU) 2016/679, které se Spojené království rozhodlo nezahrnout do GDPR Spojeného království*“.[63] Neexistence v zásadě rovnocenného ustanovení k článku 48 GDPR, které by bylo zakotveno v rámci Spojeného království pro ochranu údajů v souvislosti s předáváním nebo zveřejněním údajů, na základě rozhodnutí soudního orgánu nebo rozhodnutí správního orgánu jiné třetí země, může vést k právní nejistotě o tom, zda by úroveň ochrany osobních údajů předávaných z EHP do Spojeného království podle návrhu rozhodnutí byla zásadně ovlivněna.

101. EDPB ve svém referenčním rámci GDPR pro odpovídající ochranu v souvislosti s dalším předáváním údajů podotýká, že „*by další předávání osobních údajů příjemcem prvotního předání údajů mělo být povoleno, pouze pokud se na dalšího příjemce rovněž vztahují pravidla přiznávající odpovídající úroveň ochrany a při zpracování údajů jménem správce údajů se řídí příslušnými pokyny*“[64]. EDPB dále zdůrazňuje, že „*původní příjemce údajů předávaných z EU odpovídá za zajištění vhodných záruk pro další předávání údajů, pokud neexistuje rozhodnutí o odpovídající ochraně. Takové další předávání údajů by se mělo uskutečnit pouze pro omezené a zvláštní účely, a pokud existuje pro tento druh zpracování právní důvod*“[65]. Jako součást kapitoly V GDPR musí být článek 48 při posuzování, zda právní rámec Spojeného království zajišťuje v zásadě rovnocennou úroveň ochrany, plně zohledněn[66].

102. EDPB v této souvislosti upozorňuje na judikaturu SDEU týkající se rizika zneužití nebo protiprávního přístupu a použití údajů, a zejména uvádí, že „*pokud jde o úroveň ochrany základních práv a svobod zaručenou v rámci Unie, unijní právní předpisy obsahující zásah do základních práv zaručených články 7 a 8 Listiny musí podle ustálené judikatury Soudního dvora stanovit jasná a přesná pravidla pro rozsah a použití dotčeného opatření, která stanoví minimální požadavky, tak aby osoby, o jejichž osobní údaje se jedná, měly dostatečné záruky umožňující účinně chránit své údaje proti riziku zneužití a proti jakémukoli neoprávněnému přístupu k těmto údajům a jejich protiprávnímu využívání. Potřeba takových záruk je o to významnější v případě, kdy jsou osobní údaje zpracovávány automaticky, a existuje značné riziko neoprávněného přístupu k těmto údajům*“[67].

[63] Viz poznámka pod čarou č. 78 v návrhu rozhodnutí.
[64] Viz WP 254 rev.01, s. 6.
[65] Viz WP 254 rev.01, s. 6.
[66] Viz článek 44 GDPR, zejména poslední věta: „*Veškerá ustanovení této kapitoly se použijí s cílem zajistit, aby úroveň ochrany fyzických osob zaručená tímto nařízením nebyla znehodnocena.*“
[67] Viz Schrems I, bod 91.

103. EDPB v tomto ohledu uvádí, že na základě informací uvedených v návrhu rozhodnutí rámec Spojeného království pro ochranu údajů jasně nestanoví, že rozhodnutí soudního orgánu nebo rozhodnutí správního orgánu třetí země, jež po správci nebo zpracovateli požadují předání nebo zpřístupnění osobních údajů, lze jakýmkoli způsobem uznat nebo vymáhat, pouze pokud vycházejí z mezinárodní dohody, která je v platnosti mezi žádající třetí zemí a Spojeným královstvím. Článek 48 GDPR je zásadním ustanovením kapitoly V GDPR, neboť požaduje, aby předání či zveřejnění osobních údajů na základě rozhodnutí soudního orgánu nebo rozhodnutí správního orgánu třetí země bylo možné uznat nebo vymáhat, pouze pokud vycházejí z mezinárodní dohody, která je v platnosti mezi žádající třetí zemí a Unií nebo členským státem, aniž jsou dotčeny jiné důvody pro převod podle kapitoly V GDPR. EDPB uvádí, že „*žádost cizího orgánu není sama o sobě právním důvodem pro předání. Pořadí lze uznat, pouze pokud ‚vychází z mezinárodní dohody, například úmluvy o vzájemné právní pomoci, která je v platnosti mezi žádající třetí zemí a Unií nebo členským státem‘*“[68]. Je tudíž velmi důležité, aby v právních předpisech Spojeného království bylo možné určit v zásadě rovnocenná ustanovení.

104. V návrhu rozhodnutí Evropská komise uvádí vysvětlení orgánů Spojeného království, podle nichž je podle obyčejového práva nebo regulačních opatření cizí rozhodnutí o vyžádání údajů ve Spojeném království bez mezinárodní dohody nevynutitelné a pro jakékoli předání údajů na vyžádání cizího soudu nebo správního orgánu je nutný nástroj pro předávání, například nařízení o odpovídající ochraně nebo vhodné záruky, pokud není uplatněna výjimka podle článku 49 GDPR Spojeného království. EDPB však v tomto ohledu nebyla předložena výměna informací mezi Evropskou komisí a orgány Spojeného království[69], a tudíž není schopen provést analýzu a nezávisle posoudit, zda jsou záruky, které poskytují orgány Spojeného království, dostatečné k zajištění v zásadě rovnocenné úrovně ochrany v porovnání se zárukami uvedenými v článku 48 GDPR.

105. **EDPB vyzývá Komisi, aby poskytla další ujištění a konkrétní odkazy na právní předpisy Spojeného království, které zajistí, aby úroveň ochrany údajů podle právního rámce Spojeného království byla v zásadě rovnocenná úrovni ochrany zajištěné v EHP. EDPB tedy vyzývá Evropskou komisi, aby poskytla písemná vysvětlení a závazky orgánů Spojeného království s ohledem na provádění ochranných prostředků, které jsou v zásadě rovnocenné těm, které uvádí článek 48 GDPR.**

106. **EDPB se domnívá, že určit ustanovení v právních předpisech Spojeného království, která zajistí v zásadě rovnocennou úroveň ochrany v porovnání se zárukami uvedenými v článku 48 GDPR, je o to důležitější, že již dříve byly vyjádřeny obavy ohledně zpřístupnění údajů ve Spojeném království na žádost amerických orgánů nebo orgánů jiných třetí zemí, a s přihlédnutím k tomu, že podle rozhodnutí o odpovídající ochraně by bylo umožněno předávat údaje z EHP do Spojeného království bez jakékoli další záruky nebo závazku na straně příjemce v souvislosti s žádostmi o přístup k údajům orgány třetích zemí.**

## 3.2 Procesní a donucovací mechanismy

107. Na základě kritérií uvedených v referenčním rámci GDPR pro odpovídající ochranu provedl EDPB analýzu těchto aspektů rámce Spojeného království pro ochranu údajů, na něž se vztahuje návrh rozhodnutí: existence a účinného fungování nezávislého dozorového úřadu, existence systému zajišťujícího dobrou míru souladu s požadavky a systému zajišťujícího přístup k vhodným

[68] Viz příloha společné odpovědi EDPB a EIOÚ výboru LIBE k dopadům amerického zákona Cloud Act na evropský právní rámec pro ochranu osobních údajů, přijata dne 10. července 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[69] Viz poznámka pod čarou č. 78 v návrhu rozhodnutí.

mechanismům nápravy, které fyzickým osobám v EU poskytnou prostředky pro výkon jejich práv a domáhání se nápravy, aniž by se musely potýkat se složitými překážkami, které brání správní a soudní ochraně.

### 3.2.1 Příslušný nezávislý dozorový úřad

108. EDPB oceňuje snahu Evropské komise o komplexní posouzení zřízení, fungování a pravomocí dozorového úřadu Spojeného království v kapitole 2.6 návrhu rozhodnutí. Ve Spojeném království je úloha dohledu a vymáhání souladu s GDPR Spojeného království a zákonem DPA 2018 svěřena komisaři pro informace. Podle přílohy 12 zákona DPA 2018 je komisař pro informace „samostatným podnikem" tj. samostatnou právnickou osobou, která se skládá z jediné osoby, která je podporována úřadem ICO.

109. Pokud jde o nezávislost komisaře pro informace, EDPB zdůrazňuje, že článek 51 nařízení GDPR Spojeného království výslovně neuvádí, že je komisař pro informace nezávislým orgánem veřejné moci, jak je stanoveno v článku 51 GDPR o dozorových úřadech. EDPB přesto uznává, že GDPR Spojeného království ve svém článku 52 obdobným způsobem vychází z odpovídajících mechanismů pro nezávislost, které jsou uvedeny v čl. 52 odst. 1 až 3 GDPR.

110. EDPB dále uvádí, že článek 52 GDPR Spojeného království nestanoví povinnosti odpovídající těm v čl. 52 odst. 4 až 6 GDPR, které výslovně zajišťují, aby příslušnému dozorovému úřadu byly poskytnuty zdroje, které bude potřebovat k účinnému plnění svých úkolů a k výkonu svých pravomocí. EDPB ovšem uznává, že zákon DPA 2018 obsahuje ustanovení, jež si kladou za cíl zabezpečit vhodné financování úřadu ICO[70], včetně skutečnosti, že úřad ICO je v současné době největším dozorovým orgánem ve srovnání s dozorovými orgány v EU/EHP. Jelikož je průběžné rozdělování vhodných zdrojů, zejména pokud jde o zaměstnance a rozpočet[71], zcela nezbytné k zajištění řádného chodu dozorového úřadu, aby mohl plnit všechny své přidělené úkoly, a které rovněž bylo Evropským parlamentem nedávno označeno jako „zásadní"[72], považuje EDPB za nezbytné věnovat zvláštní pozornost budoucímu vývoji v této oblasti.

111. **EDPB tudíž vyzývá Evropskou komisi, aby sledovala veškerý vývoj v oblasti rozdělování zdrojů úřadu ICO, který by mohl mít neblahý vliv na řádné plnění úkolů úřadu.**

### 3.2.2 Existence systému pro ochranu údajů zajišťujícího dobrou míru souladu s požadavky

112. V návrhu rozhodnutí je provedeno komplexní posouzení pravomocí, které jsou svěřeny úřadu ICO podle článku 58 GDPR Spojeného království a zákona DPA 2018, aby bylo zajištěno monitorování právních předpisů a jejich prosazování. EDPB uznává, že článek 58 GDPR Spojeného království vychází obdobným způsobem z odpovídajících mechanismů, které se týkají pravomocí dozorových úřadů, jak je uvedeno v článku 58 GDPR. Pokud jde o pravomoc uložit správní pokuty v závislosti na okolnostech každého jednotlivého případu, článek 83 GDPR Spojeného království obsahuje podobná ustanovení a maximální výše jako článek 83 GDPR. EDPB se tudíž domnívá, že právní rámec Spojeného království je v této oblasti aktuálně v souladu s normami, které jsou stanoveny v příslušných právních předpisech EU. V této souvislosti ovšem EDPB zdůrazňuje, že zavedení *účinných* sankcí hraje důležitou úlohu při zajištění respektování pravidel.[73]

[70] Viz články 137, 138, 182 a článek 9 přílohy 12 zákona DPA 2018.
[71] Viz WP 254 rev.01, s. 7.
[72] Usnesení Evropského parlamentu ze dne 25. března 2021 o hodnoticí zprávě Komise o provádění obecného nařízení o ochraně osobních údajů dva roky od začátku jeho uplatňování, bod 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_CS.html.
[73] Viz WP 254 rev.01, s. 7.

113. **S ohledem na výše uvedené EDPB vyzývá Evropskou komisi, aby sledovala účinnost sankcí a příslušných nápravných opatření v rámci Spojeného království pro ochranu údajů.**

#### 3.2.3 Systém pro ochranu údajů musí subjektům údajů poskytovat podporu a pomoc při uplatňování jejich práv a zajišťovat vhodné mechanismy nápravy

114. Účinný mechanismus dohledu, který umožní nezávislé prověřování stížností s cílem určit porušování práv subjektů údajů a v praxi jej trestat, jakož i účinná správní a soudní ochrana (včetně náhrady škody za protiprávní zpracování osobních údajů subjektu údajů), jsou klíčovými prvky posouzení, zda systém pro ochranu údajů poskytuje vhodnou úroveň ochrany.

115. EDPB oceňuje, že úřad ICO poskytuje na svých internetových stránkách komplexní informace a pokyny, jejichž cílem je zvýšit povědomí správců a zpracovatelů údajů o jejich povinnostech, a zároveň se snaží podpořit subjekty údajů v informovanosti o jejich právech s ohledem na osobní údaje a uplatňování jednotlivých práv podle GDPR Spojeného království a zákona DPA 2018.

116. **Bez ohledu na aktuální stav EDPB vyzývá Evropskou komisi, aby průběžně sledovala úroveň podpory, kterou úřad ICO poskytuje, a to zejména osobám, jejichž osobní údaje jsou předávány ze Spojeného království podle rozhodnutí o odpovídající ochraně, aby jim bylo umožněno uplatňovat svá práva podle právní úpravy Spojeného království.**

# 4. PŘÍSTUP ORGÁNŮ VEŘEJNÉ MOCI K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM Z EU A JEJICH POUŽITÍ TĚMITO ORGÁNY VE SPOJENÉM KRÁLOVSTVÍ

## 4.1 Přístup britských orgánů veřejné moci k osobním údajům a jejich použití těmito orgány pro účely prosazování trestního práva

### 4.1.1 Právní základ a použitelná omezení/záruky

117. Pokud jde o posouzení **přístupu k údajům pro účely vymáhání práva**, jež Evropská komise provedla a doložila ve 132. a následujících bodech odůvodnění návrhu rozhodnutí, uvádí Evropská komise diferencované a podrobné informace a obecně vyvozuje srozumitelné závěry. EDPB proto v tomto stanovisku upustil od opakování většiny faktických zjištění a hodnocení. V některých případech ovšem není zachycení skutečností nebo vysvětlení závěrů dostačující, aby je EDPB mohl přijmout.

#### 4.1.1.1 Používání souhlasu

118. EDPB bere na vědomí, že Evropská komise v poznámce pod čarou č. 184 v návrhu rozhodnutí[74] tvrdí, že **používání souhlasu** není v rámci posuzování shody podstatné, jelikož v případě předávaných údajů nezískává orgán pro vymáhání práva ve Spojeném království tyto údaje přímo od subjektu údajů na základě souhlasu. Používání souhlasu jako právního základu pro vynucování práva tudíž Evropská komise neposuzuje.

119. EDPB v tomto ohledu připomíná, že čl. 45 odst. 2 písm. a) GDPR požaduje posouzení široké škály prvků, které se nevztahují na situace předávání údajů, například „*právní stát, dodržování lidských práv a základních svobod, příslušné právní předpisy, obecné i odvětvové, včetně […] trestního práva*“.

[74] Viz s. 37 návrhu rozhodnutí.

120. EDPB na základě informací rovněž poskytnutých Evropskou komisí v 38. bodě odůvodnění návrhu prováděcího rozhodnutí v souladu se směrnicí Evropského parlamentu a Rady (EU) 2016/680 o odpovídající ochraně osobních údajů ve Spojeném království (dále jen „návrh rozhodnutí o odpovídající ochraně LED“) uvádí, že použití souhlasu, jak je popisováno v režimu Spojeného království pro oblast prosazování práva, by se vždy mělo spoléhat na právní základ. To znamená, že i když má policie v některých případech zákonnou pravomoc zpracovávat údaje pro účely vyšetřování (například sběr vzorku DNA), může považovat za správné požádat subjekt údajů o svolení.

121. **EDPB vyzývá Evropskou komisi, aby do rozhodnutí o odpovídající ochraně zanesla svou analýzu možného použití souhlasu v oblasti prosazování práva, které je uvedeno v návrhu rozhodnutí o odpovídající ochraně LED.**

#### 4.1.1.2 Příkazy k domovní prohlídce a předávací příkazy

122. Ačkoli EDPB nemá obecně žádné připomínky ke způsobu získávání důkazů policií pomocí příkazů k domovní prohlídce a předávacích příkazů, ze 136. bodu odůvodnění návrhu rozhodnutí vyplývá, že Evropská komise zaměřila své úvahy o přístupu k údajům pro účely vymáhání práva na policii, a zpracování údajů jinými donucovacími orgány bylo hodnoceno v menší míře.

123. Například dokument Spojeného království „Explanatory Framework for Adequacy Discussions“, oddíl F: Prosazování práva[75], na straně 11 uvádí, že **Národní agentura pro boj proti trestné činnosti** (NCA) by obzvláště mohla sloužit jako donucovací orgán, jelikož plní mimo jiné obecnou funkci zpravodajství o trestné činnosti. Agentura NCA své poslání popisuje jako shromažďování informací z různých zdrojů s cílem maximalizovat analýzu, hodnocení a taktické příležitosti, včetně informací získávaných z technického zachycování komunikace, od partnerů v oblasti prosazování práva ve Spojeném království i v zahraničí a od bezpečnostních a zpravodajských agentur[76]. Agentura NCA je také jedním z hlavních partnerů v oblasti prosazování práva a hraje důležitou úlohu při výměně informací kriminálního zpravodajství[77].

124. EDPB dále zohledňuje skutečnost, že vládní komunikační ústředí (Government Communications Headquarters, GCHQ), jehož činnosti obvykle spadají do oblasti působnosti části 4 zákona DPA 2018,

---

[75] Viz vládní dokument Spojeného království „Explanatory Framework for Adequacy Discussions“, oddíl F: Prosazování práva, 13. března 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Viz internetové stránky Národní agentury pro boj proti trestné činnosti, Zpravodajství: posílení obrazu závažné organizované trestné činnosti ve Spojeném království, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Ačkoli se veškeré zprávy zpracovávané agenturou NCA netýkají osobních údajů, u podstatné části tomu tak je, navíc se popsané činnosti liší od činností standardního policejního dohledu, tudíž by posouzení přístupu k osobním údajům donucovacími orgány ve Spojeném království nebylo úplné bez řádného posouzení činností agentury NCA. Zdá se vhodné zajistit, aby zásadám v oblasti ochrany údajů byl přikládán stejný význam ve všech příslušných orgánech pro vymáhání práva, a upozornit tak na agenturu obzvláště založenou na datech, jakou je agentura NCA. Kromě toho „s výhledem do budoucna“, jak se dále uvádí ve vysvětlení, „*[s]e neustále snažíme o vyhledávání nových příležitostí pro shromažďování, vývoj a posílení tradičních schopností, aby byla zvýšena kvantita a kvalita zpráv dostupných k využití jak ve Spojeném království, tak v zahraničí*“. „*V rámci toho vyvíjíme novou schopnost využití vnitrostátních údajů použitím pravomocí, které byly agentuře svěřeny zákonem o trestných činech a soudech, abychom získali přístup k údajům uchovávaných ve veřejné správě a společně je propojili a využili.*“ […] „*Toto vše přispěje ke zvýšení naší pohotovosti a flexibilitě reagovat na nové hrozby a aktivně fungovat, abychom shromáždili informace a zprávy o nových hrozbách a provedli jejich analýzu s cílem zasáhnout dříve, než se tyto hrozby naplní.*“

tj. národní bezpečnosti, rovněž sehrává aktivní úlohu při snižování společenské a finanční újmy, kterou závažná a organizovaná trestná činnost způsobuje ve Spojeném království, v úzké spolupráci s ministerstvem vnitra, agenturou NCA, úřadem HM Revenue and Customs (HRMC) a dalšími vládními úřady[78]. Jeho činnosti se týkají boje proti pohlavnímu zneužívání dětí; podvodů; dalších druhů hospodářské trestné činnosti, včetně legalizace výnosů z trestné činnosti; trestného zneužívání technologií; kyberkriminality; organizované trestné činnosti týkající se přistěhovalectví, včetně obchodování s lidmi; drog, palných zbraní a další činnosti nezákonného převaděčství.

125. **EDPB vyzývá Evropskou komisi, aby doplnila svou analýzu o analýzu orgánů činných v oblasti vymáhání práva, u nichž se zdá, že zařadily shromažďování a analýzu údajů, včetně osobních údajů, na seznam svých hlavních každodenních činností, zejména agentura NCA. EDPB dále vyzývá Komisi, aby se blíže zaměřila na orgány, jako ústředí GCHQ, jejichž činnosti spadají jak do oblasti působnosti vymáhání práva a vnitrostátní bezpečnosti, tak do právního rámce, který se na ně vztahuje v případě zpracování osobních údajů.**

#### 4.1.1.3 Vyšetřovací pravomoci pro účely prosazování práva

126. V kapitole 4 referenčního rámce GDPR pro odpovídající ochranu nazvané „Základní záruky přístupu pro účely **prosazování práva** a národní bezpečnosti **ve třetích zemích**, kterými se omezuje zásah do základních práv“ EDPB uvádí, že *„[v] této souvislosti Soudní dvůr rovněž kriticky připomněl, že rozhodnutí podle zásady bezpečného přístavu ‚neobsahuje žádné zjištění ohledně existence pravidel státního charakteru ve Spojených státech, jež mají omezit případné zásahy do základních práv osob, jejichž osobní údaje jsou předávány z Unie do Spojených států, tj. **zásahy, jež by státní subjekty této země byly oprávněny činit v případě, že sledují takové legitimní cíle**, jako je bezpečnost státu“*[79]. V tomto rámci EDPB uvádí, že **má-li se přístup k údajům považovat za odpovídající, je třeba, aby všechny třetí země**, ať už pro účely národní bezpečnosti nebo prosazování práva, **dodržovaly čtyři základní evropské záruky**[80], zejména **je nutné prokázat jeho nezbytnost a přiměřenost ve vztahu ke sledovaným legitimním cílům**.

127. V této části návrhu rozhodnutí Evropská komise uvádí (139. bod odůvodnění), že *„jelikož jsou vyšetřovací pravomoci uvedené v zákoně IPA 2016 totožné s těmi, které jsou dostupné vnitrostátním bezpečnostním agenturám, zabývá se jejich podmínkami, omezeními a zárukami podrobněji oddíl o přístupu britských orgánů veřejné moci k osobním údajům a jejich použití těmito orgány pro účely národní bezpečnosti*“. Z judikatury SDEU ovšem vyplývá, že legitimní cíle, například národní bezpečnost nebo boj proti závažným trestným činům, jsou při uplatnění zkoušky potřebnosti a přiměřenosti na právní předpisy členských států, jež umožňují orgánům veřejné moci přistupovat k osobním údajům a uchovávat je, rozdílné, a tudíž by bylo možné v určitém případě ospravedlnit některý druh zásahu, zatímco v jiném nikoliv[81].

128. **EDPB by v rozhodnutí tedy ocenil konkrétní posouzení nezbytnosti a přiměřenosti podmínek, omezení a záruk popsaných ve 174. a následujících bodech odůvodnění (což je oddíl věnovaný opatřením, která sledují cíle národní bezpečnosti), pokud jde o uplatňování těchto podmínek, omezení a záruk v souvislosti s opatřeními, která sledují cíle prosazování práva. Vyzývá proto**

[78] Viz internetové stránky ústředí GCHQ, Mise, Závažná a organizovaná trestná činnost, https://www.gchq.gov.uk/section/mission/serious-crime.
[79] Viz WP 254 rev.01, s. 9.
[80] Viz doporučení EDPB 02/2020 týkající se evropských základních záruk pro sledovací opatření.
[81] Viz rozsudek SDEU ze dne 6. října 2020, La Quadrature du Net a další, spojené věci C-511/18, C-512/18 a C-520/18, ECLI:EU:C:2020:791.

**Evropskou komisi, aby dále objasnila, zda je popsané uchovávání osobních údajů a jejich zpřístupnění pro účely vymáhání práva dostatečně omezeno, aby byla úroveň ochrany údajů v zásadě rovnocenná úrovni ochrany zajištěné v EU.**

### 4.1.2 Další použití údajů shromažďovaných pro účely prosazování práva (140. až 154. bod odůvodnění)

129. V souvislosti s dalším použitím údajů shromážděných pro účely prosazování práva EDPB uvádí, že rámec Spojeného království pro ochranu údajů poskytuje podobné záruky a podobná omezení jako unijní právní řád.

#### 4.1.2.1 Další použití pro ostatní účely prosazování práva

130. Zákon DPA 2018 stanoví, že osobní údaje shromážděné příslušným orgánem pro účely prosazování práva mohou být dále zpracovány (ať už původním správcem, nebo dalším správcem) pro jiný účel prosazování práva, pokud je správce k tomuto druhu zpracovávání ze zákona oprávněn a zpracování je pro tento účel potřebné a přiměřené. Evropská komise uvádí, že se všechny záruky uvedené v části 3 zákona DPA 2018 vztahují na zpracování údajů prováděné přijímajícím orgánem. EDPB však zdůrazňuje, že čl. 44 odst. 4, čl. 45. odst. 4, čl. 48 odst. 3 a čl. 68 odst. 7 části 3 zákona DPA 2018 umožňují omezení práva subjektu údajů a článek 79 umožňuje vydání osvědčení, které dokládá, že omezení je potřebným a přiměřeným opatřením na ochranu národní bezpečnosti. **EDPB tedy doporučuje, aby Evropská komise dále posoudila možný dopad těchto omezení na úroveň ochrany osobních údajů v souvislosti s dalším použitím shromážděných údajů. Obdobně je třeba blíže upřesnit právní rámec Spojeného království, který takové další sdílení údajů umožňuje, zejména zákon o digitální ekonomice z roku 2017 (Digital Economy Act 2017) a zákon o trestných činech a soudech z roku 2013 (Crime and Courts Act 2013), který umožňuje sdílení údajů s agenturou NCA.**

#### 4.1.2.2 Další použití pro jiné účely než účely prosazování práva ve Spojeném království

131. Zákon DPA 2018 rovněž stanoví, že osobní údaje shromážděné pro účely prosazování práva mohou být zpracovány pro jiný účel než prosazování práva, pokud takové zpracování údajů povoluje zákon. V tomto případě tvoří právní základ, který opravňuje k takovému sdílení údajů, článek 19 protiteroristického zákona z roku 2008 (Counter-Terrorism Act 2008). EDPB v této souvislosti uvádí, že oblast působnosti a ustanovení článku 19 protiteroristického zákona nejsou v posouzení Evropskou komisí plně zohledněny a může z nich vyplývat další použití obecnější povahy, zejména s ohledem na čl. 19 odst. 2, který uvádí, že „*[ú]daje, které získá zpravodajská služba při výkonu své činnosti, může tato služba použít k výkonu svých dalších činností*“.

132. EDPB rovněž podotýká, že by zmínka Evropské komise o tom, že příslušnými orgány jsou orgány veřejné moci, které musí jednat v souladu s EÚLP včetně článku 8 této úmluvy, aby bylo zajištěno, že sdílení údajů mezi orgány pro vymáhání práva a zpravodajskými službami probíhá v souladu s právními předpisy pro ochranu osobních údajů a v souladu s EÚLP, mohla být dále podložena stanovením příslušných zákonů a předpisů právního řádu Spojeného království, které jasně a přesně taková omezení stanovují.

#### 4.1.2.3 Další použití s ohledem na další předávání údajů mimo Spojené království

133. Ačkoli Evropská komise uvedla, že dohoda podle zákona CLOUD Act mezi Spojeným královstvím a USA může ovlivnit další předávání údajů do USA od poskytovatelů SEK ve Spojeném království, EDPB rovněž zdůrazňuje, že vstup této dohody v platnost může rovněž ovlivnit další použití údajů, které orgány pro vymáhání práva ve Spojeném království získají z dalšího předávání údajů, zejména v

souvislosti s vydáváním a převáděním příkazů podle článku 5 dohody podle zákona CLOUD Act mezi Spojeným královstvím a USA.

134. Obecně se EDPB domnívá, že uzavírání budoucích dvoustranných dohod se třetími zeměmi pro účely spolupráce zpravodajských služeb, jež poskytne právní základ pro předávání osobních údajů do třetích zemí, může rovněž významně ovlivnit podmínky dalšího použití shromážděných údajů, jelikož tyto dohody mohou mít dopad na posuzovaný rámec Spojeného království pro ochranu údajů. EDPB tedy doporučuje, aby Evropská komise dále tento bod zhodnotila a určila, zda mezinárodní dohody existují, a objasnila, zda ustanovení těchto dohod mohou ovlivnit použití právních předpisů Spojeného království pro ochranu údajů a zda stanoví další omezení nebo výjimky související s dalším použitím a zahraničním zpřístupněním údajů, které byly shromážděny pro účely prosazování práva. EDPB se domnívá, že takové informace a hodnocení jsou klíčové, aby bylo možné provést komplexní posouzení úrovně ochrany přiznané právním rámcem Spojeného království a jeho postupů, které se týkají zpřístupnění a dalšího použití údajů v zahraničí.

#### 4.1.3 Dozor

135. EDPB uvádí, že dohled orgánů pro vymáhání práva je kromě úřadu ICO zajišťován prostřednictvím různých komisařů. V návrhu odpovídající úrovně ochrany je uveden komisař IPC, komisař pro uchovávání a využití biometrických materiálů a komisař pro sledovací zařízení. V tomto ohledu je důležité podotknout, že SDEU opakovaně zdůraznil potřebu nezávislého dohledu. V otázce přístupu k osobním údajům předávaným do Spojeného království je obzvláště důležitý komisař IPC. EDPB má za to, že komisař IPC je tzv. „soudním komisařem“, stejně jako ostatní soudní komisaři, na které se odkazuje v kapitole o národní bezpečnosti, a že tito soudní komisaři požívají výhod nezávislosti soudců, a to i když vykonávají funkci komisaře. Pokud jde o úřad komisaře IPC, Evropská komise v 245. bodě odůvodnění návrhu rozhodnutí vysvětluje, že funguje nezávisle jako nezávislá veřejná instituce a financuje jej ministerstvo vnitra.

136. EDPB v návrhu rozhodnutí nenalezl další potřebné informace k posouzení nezávislosti komisaře pro uchovávání a využití biometrických materiálů ani komisaře pro sledovací zařízení.

137. **Evropská komise se vyzývá, aby dále posoudila nezávislost soudních komisařů, a to rovněž v případech, kdy komisař (již) nevykonává funkci soudce, včetně posouzení nezávislosti komisaře pro uchovávání a využití biometrických materiálů a komisaře pro sledovací zařízení.**

### 4.2 Obecný právní rámec pro ochranu údajů v oblasti národní bezpečnosti

#### 4.2.1 Národní bezpečnostní osvědčení

138. Podle článku 111 zákona DPA 2018 mohou správci požádat o vydání národního bezpečnostního osvědčení, jež vydává ministr, člen kabinetu, generální prokurátor nebo generální advokát pro Skotsko, která potvrzují, že výjimky z práv a povinností zakotvených v částech 4 až 6 zákona DPA 2018 jsou potřebným a přiměřeným opatřením na ochranu národní bezpečnosti. Tato osvědčení slouží k tomu, aby správcům zajistila větší právní jistotu, a zároveň jsou nezvratným důkazem, že národní bezpečnost lze při zpracování osobních údajů uplatnit. Je však třeba poznamenat, že tato osvědčení

nejsou pro uplatnění výjimky z důvodu národní bezpečnosti nutná, ale slouží spíše jako opatření transparentnosti[82].

139. EDPB podle článků 17 a 18 přílohy 20 zákona DPA 2018 zjistil, že národní bezpečnostní osvědčení vydané podle zákona o ochraně údajů z roku 1998 (dále jen „staré osvědčení“) mělo prodlouženou platnost pro zpracování osobních údajů podle zákona DPA 2018 do 25. května 2019. Do dnešního dne se osvědčení, která nebyla nahrazena nebo zrušena, považovala za osvědčení vydaná podle zákona DPA 2018.

140. Pokud na národním bezpečnostním osvědčení vydaném podle zákona o ochraně údajů z roku 1998 však není uvedeno konkrétní datum platnosti, EDPB předpokládá, že takové osvědčení zůstane v souvislosti se zpracováním údajů podle zákona o ochraně údajů z roku 1998 v platnosti, dokud nebude zrušeno nebo prohlášeno za neplatné[83]. Ačkoli je ochrana poskytovaná těmito starými osvědčeními omezená na zpracování údajů podle zákona o zpracování údajů z roku 1998, EDPB uvádí, že podle tohoto zákona lze v případě osobních údajů, které byly podle něj zpracovány, vydávat nová národní bezpečnostní osvědčení.[84]

141. **EDPB vyzývá Evropskou komisi, aby ve svém návrhu rozhodnutí pro úplnost uvedla, že národní bezpečnostní osvědčení lze stále vydávat podle zákona o ochraně údajů z roku 1998. Kromě toho EDPB vyzývá Evropskou komisi, aby ve svém návrhu rozhodnutí popsala mechanismy nápravy a dohledu týkající se osvědčení vydaných podle zákona o ochraně údajů z roku 1998. A konečně EDPB vyzývá Evropskou komisi, aby ve svém návrhu rozhodnutí uvedla počet existujících osvědčení, která byla vydána podle zákona o ochraně údajů z roku 1998, a pozorně tuto situaci sledovala.**

### 4.2.2 Právo na opravu a výmaz

142. Pokud jde o právo na opravu a výmaz, EDPB bere na vědomí, že v souladu s článkem 100 a článkem 149 zákona DPA 2018 mají subjekty údajů možnost spolehnout se na Vrchní soud (ve Skotsku na Nejvyšší civilní soud), aby správci údajů nařídil neprodleně opravit či vymazat jejich údaje.

143. **EDPB zdůrazňuje, že uplatňování práv subjektů údajů musí být účinně zajištěno, a tudíž vyzývá Evropskou komisi, aby ve svém návrhu rozhodnutí popsala, jak článek 100 zákona DPA 2018 funguje v praxi, a podrobně sledovala jeho uplatňování.**

### 4.2.3 Výjimky z důvodu státní bezpečnosti

144. EDPB by rád upozornil na článek 110 zákona DPA 2018 a zejména přílohu 11, která stanoví konkrétní účely, kvůli kterým se zpravodajské služby mohou odchýlit od některých zásad ochrany údajů, včetně práv subjektů údajů, a nemají povinnost nahlašovat porušování osobních údajů úřadu ICO.[85]

[82] Viz dokument ministerstva vnitra „The Data Protection Act 2018, National Security Certificates guidance“, srpen 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] Viz dokument ministerstva vnitra „The Data Protection Act 2018, National Security Certificates guidance“, srpen 2020, s. 5.

[84] Viz dokument ministerstva vnitra „The Data Protection Act 2018, National Security Certificates guidance“, srpen 2020, bod 8, s. 5.

[85] Těmito účely jsou: předcházení a odhalování „trestné činnosti“, „informace, jejichž zveřejnění je vyžadováno ze zákona nebo v souvislosti se soudním řízením“, „parlamentní výsady”, „soudní řízení”, „státní pocty a vyznamenání“, „ozbrojené síly“, „hospodářský blahobyt“, „povinnost mlčenlivosti“, „vyjednávání”, „důvěrné

145. **EDPB vyzývá Evropskou komisi, aby dále objasnila rozsah výjimek, jelikož jej zajímá, zda jsou všechny výjimky uvedené v příloze 11 zákona DPA 2018 pro práci zpravodajských služeb podstatné a zda zajišťují shodu se zásadou nezbytnosti a proporcionality.** EDPB především **vyzývá Evropskou komisi, aby uvedla podrobnější informace o tom, za jakých okolností by se zpravodajská služba mohla spolehnout na článek 10 přílohy 11 zákona DPA 2018, který uvádí, že *„[u]vedená ustanovení se nevztahují na osobní údaje, které tvoří záznamy o záměru správce zahájit se subjektem údajů jakékoli jednání, pokud by uplatnění uvedených ustanovení pravděpodobně tato jednání ohrozilo*“.**

## 4.3 Přístup britských orgánů veřejné moci k osobním údajům a jejich použití těmito orgány pro účely národní bezpečnosti

146. Obecně EDPB podotýká, že jsou státům v záležitostech národní bezpečnosti ponechány široké posuzovací pravomoci, což uznává i ESLP. EDPB rovněž připomíná, jak zdůrazňuje ve svém aktualizovaném doporučení týkajícím se evropských základních záruk pro sledovací opatření[86], že čl. 6 odst. 3 Smlouvy o Evropské unii stanoví, že základní práva, která jsou zakotvena v EÚLP, jsou součástí práva unie jakožto obecné zásady. Jak ovšem připomíná SDEU ve své judikatuře, uvedená úmluva nepředstavuje právní nástroj formálně začleněný do práva Unie, dokud k ní Unie nepřistoupí[87]. Úroveň ochrany základních práv vyžadovaná v článku 45 GDPR musí být určena na základě ustanovení téhož nařízení ve spojení se základními právy zaručenými Listinou EU. V tomto ohledu mají podle čl. 52 odst. 3 Listiny EU v ní obsažená práva odpovídající právům zaručeným EÚLP stejný smysl a stejný rozsah, jaký jim přikládá EÚLP. Jak připomíná SDEU, judikatura ESLP týkající se práv, která jsou rovněž uvedena v Listině EU, tudíž musí být zohledněna jako minimální úroveň ochrany pro výklad odpovídajících práv v Listině EU[88]. Podle poslední věty čl. 52. odst. 3 Listiny EU to však *„[n]ebrání tomu, aby právo Unie poskytovalo širší ochranu*“.

147. V následujícím posouzení tudíž EDPB zohlednil judikaturu ESLP v tom smyslu, že Listina EU, tak jak ji vykládá SDEU, nestanoví vyšší úroveň ochrany ukládající jiné požadavky než judikatura ESLP.

### 4.3.1 Právní základy, omezení a záruky – vyšetřovací pravomoci vykonávané v rámci národní bezpečnosti

#### 4.3.1.1 Obecné poznámky

148. EDPB připomíná, že zákon IPA 2016 je nedávno přijatým právním předpisem, který změnil několik ustanovení zákona o zpravodajských službách z roku 1994. Zákon stanoví, do jaké míry mohou být některé vyšetřovací pravomoci použity při zásahu do soukromí[89]. Kromě dvou zpráv komisaře IPC, které uvádějí užitečné informace o uplatnění tohoto nového právního rámce, stále chybí hodnocení některých aspektů, zejména používaných selektorů a vyhledávacích kritérií.

149. Dále EDPB obecně k zákonu IPA 2016 a jeho oblasti působnosti uvádí tyto čtyři body, jimž je potřeba věnovat pozornost:

odkazy poskytnuté správcem“, „zkouškové testy a hodnocení“, „výzkum a statistiky“ a „archivace ve veřejném zájmu“.

[86] Viz doporučení EDPB 02/2020 týkající se evropských základních záruk pro sledovací opatření.

[87] Viz Schrems II, bod 98.

[88] Viz rozsudek SDEU ze dne 6. října 2020, La Quadrature du Net a další, spojené věci C-511/18, C-512/18 a C-520/18, ECLI:EU:C:2020:791, bod 124.

[89] Viz článek 1 zákona IPA 2016.

150. U **prvního bodu**, který se týká charakteristiky právních předpisů, by EDPB rád poukázal na dvě souvislosti:

151. Nejprve EDPB uvádí, že právní předpisy odkazují na obecné účely použití postupů uvedených v zákoně IPA 2016, a nikoliv na kategorie osob, kterých se shromažďování údajů může týkat na základě částí 2 až 7 zákona IPA 2016. V tomto ohledu EDPB připomíná, že by měla existovat spojitost mezi kategoriemi osob, které mohou podléhat sledovacím opatřením, a mezi účely, které právní předpisy stanoví pro vymezení osobní působnosti práva.

152. EDPB dále zdůrazňuje, že definice „telekomunikační operátoři", „telekomunikační služba" a „telekomunikační systém", které vymezují působnost práva, jsou rovněž velmi obecné a do jisté míry nejasné. EDPB upozorňuje, že tyto pojmy musí být v oblasti zákona IPA 2016 chápány v mnohem širším smyslu než v případě právních předpisů o telekomunikaci, jak je uvedeno například v evropském kodexu pro elektronické komunikace[90]. EDPB uvádí, že definice „telekomunikační služba" a „telekomunikační systém" jsou v zákoně údajně záměrně uváděny v obecné rovině, aby zůstaly platné i pro nové technologie. Stejně tak je velmi obecná definice „telekomunikační operátor", což by mohlo zahrnovat například on-line videohry se zabudovaným prvkem „chatu" nebo jiné internetové stránky, které mají pouhá „chatovací" okénka[91].

153. Ačkoli jsou v právních předpisech obecně stanoveny postupy a dohled týkající se posouzení nezbytnosti a přiměřenosti přístupu k údajům a jejich shromažďování, kritéria určující, jak takové hodnocení provádět, v samotných právních předpisech vymezena nejsou. Další informace lze nalézt v jiných dokumentech, například v kodexech.

154. Jak ovšem připomíná doporučení EDPB 02/2020 týkající se evropských základních záruk pro sledovací opatření, SDEU uvedl, že *„požadavek, aby každé omezení výkonu základních práv bylo stanoveno zákonem, implikuje, že právní základ dovolující zásah do těchto práv musí sám definovat rozsah omezení výkonu dotyčného práva"*[92]. Konkrétněji SDEU uvedl, že *„za účelem splnění požadavku proporcionality musí právní úprava stanovit jasná a přesná pravidla pro rozsah a použití předmětného opatření a stanovit minimální požadavky, tak aby osoby, o jejichž osobní údaje jde, měly dostatečné záruky umožňující účinně chránit tyto údaje před rizikem zneužití. Tato právní úprava musí být právně závazná ve vnitrostátním právu a musí zejména vymezit okolnosti a podmínky, za nichž může být přijato opatření týkající se zpracovávání takových údajů, čímž zaručí, že se zásah omezí na to, co je nezbytně nutné."*[93]

[90] Viz čl. 2 odst. 5 evropského kodexu pro elektronické komunikace, ve kterém je například „interpersonální komunikační služba" definována jako *„služba obvykle poskytovaná za úplatu, která prostřednictvím sítí elektronických komunikací umožňuje přímou interpersonální a interaktivní výměnu informací mezi konečným počtem osob, kdy osoby, které komunikaci zahajují nebo se jí účastní, určují jejího/její příjemce a která nezahrnuje služby, které interpersonální a interaktivní komunikaci umožňují pouze jako nepodstatnou pomocnou funkci, která je ze své podstaty spjata s jinou službou*".

[91] Viz dokument ministerstva vnitra „Code of Practice on the Interception of Communications", březen 2018, bod 2.5 a následující, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Viz Schrems II, bod 175. a citovaná judikatura, jakož i rozsudek SDEU ze dne 6. října 2020, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs a další, C-623/17, ECLI:EU:C:2020:790 (dále jen „Privacy International"), bod 65.

[93] Viz Privacy International, bod 68.

155. ESLP rovněž zdůraznil význam jasnosti práva, které by mělo jednotlivcům poskytnout „*odpovídající představu o okolnostech a podmínkách, za kterých jsou orgány veřejné moci oprávněny taková opatření přijmout*“[94].

156. **EDPB tedy vyzývá Evropskou komisi, aby dále zhodnotila tyto aspekty týkající se přesnosti, jasnosti a úplnosti příslušných právních předpisů a aby uvedla další informace, které prokáží, že tyto předpisy poskytují úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany zajištěné v EU, s ohledem na charakteristiku právních předpisů. EDPB dále zdůrazňuje, že by měly být zhodnoceny obecné definice související s přiměřeností opatření v oblasti zachycování údajů.**

157. Ačkoli jsou v několika interních kodexech příslušných orgánů zpravodajské komunity některé tyto prvky částečně rozvinuty, například posouzení nezbytnosti a přiměřenosti shromažďování údajů, EDPB zdůrazňuje, že požadavky SDEU s ohledem na povahu právního řádu předpokládají, že základní prvky, jako možnost osob spolehnout se na opravné prostředky, musí být uvedeny v právních předpisech, které stanoví vymahatelná práva[95]. V článku 6 přílohy 7 zákona IPA 2016 se uvádí, že soudy (a dozorové úřady) „*při rozhodování ve věcech v rámci řízení přihlížejí k tomu, že se osoba opomněla řídit kodexem*“, aniž by bylo uvedeno, zda jednotlivci mohou před soudy (nebo dozorovými úřady) porušení kodexů vymáhat. Informace, které byly dosud uvedeny v návrhu rozhodnutí, buď odkazují na uznání předvídatelnosti pravidel uvedených v těchto kodexech ze strany ESLP[96], spíše než na jejich „žalovatelnost“ u soudu, jak požaduje SDEU, nebo na skutečnost, že soudy Spojeného království v některých případech odkázaly na kodexy, přičemž žádný z uvedených případů názorně neukázal, jakým způsobem mohou jednotlivci práva odvozená z těchto kodexů uplatňovat. **Dojde-li se k závěru, že právní předpisy Spojeného království dostatečně neuvádějí okolnosti a podmínky, za kterých lze přijmout opatření, a že tyto informace jsou ve skutečnosti uvedeny v interních kodexech orgánů zpravodajské komunity, pak EDPB vyzývá Evropskou komisi, aby dále posoudila, zda omezení a záruky uvedené v různých interních kodexech orgánů komunikačního zpravodajství mohou jednotlivci uplatňovat u soudu a vymáhat je.**

158. **Druhý bod** se týká skutečnosti, že se ustanovení, která se týkají cíleného získávání a uchovávání komunikačních údajů na jedné straně a hromadného shromažďování na straně druhé, ať už v zákoně IPA 2016, nebo v jiných právních předpisech, například v zákoně o zpravodajských službách z roku 1994 nebo v nařízení k zákonu o vyšetřovacích pravomocích z roku 2000, budou rovněž vztahovat na údaje předávané z EU do Spojeného království. Pokud jde o hromadné shromažďování, EDPB zdůrazňuje, že příslušná ustanovení právních předpisů Spojeného království umožňují shromažďování údajů mimo Spojené království, což by mohlo zahrnovat údaje na cestě předávané z EHP do Spojeného království na základě rozhodnutí o odpovídající ochraně[97]. Dále si EDPB všímá, že Evropská komise uvádí, že „*[j]e třeba poznamenat, že uchovávání a získávání údajů z komunikace se běžně netýká osobních údajů subjektů údajů z EU, které jsou předávány podle tohoto rozhodnutí do Spojeného království. Povinnost uchovat a zveřejnit údaje z komunikace podle části 3 a 4 zákona IPA 2016 se vztahuje na údaje, které jsou shromažďovány telekomunikačními operátory ve Spojeném*

[94] Viz rozsudek ESLP ze dne 4. prosince 2015, Zakharov v. Russia, CE:ECHR:2015:1204JUD004714306, bod 229.
[95] V této souvislosti SDEU například uvážil, že americká směrnice PPD-28 neobstála, ačkoli stanovila některá omezení týkající se hromadného shromažďování údajů, viz Schrems II, bod 181.
[96] Viz rozsudek ESLP ze dne 13. září 2018, Big Brother Watch a další v. Spojené království, ECLI:CE:ECHR:2018:0913JUD005817013 (dále jen „Big Brother Watch“), bod 325: „*Jelikož je kodex ‚the IC Code‘ veřejným dokumentem, který podléhá schválení obou komor Parlamentu, a musí být zohledněn jak osobami, které vykonávají služby zachytávání informací, tak soudy a tribunály, Soudní dvůr výslovně uznal, že jeho ustanovení lze vzít v úvahu při posuzování předvídatelnosti režimu zákona RIPA*.“
[97] Viz bod 183 a následující rozsudku Schrems II o posouzení právních předpisů, které stanovují přístup k údajům na cestě mezi EU a třetí zemí v souvislosti s rozhodnutím o odpovídající ochraně.

*království přímo od uživatelů telekomunikačních služeb.*“[98] EDPB ovšem upozorňuje na nejasnost, která panuje okolo skutečnosti, že žádosti od příslušných orgánů Spojeného království mohou obdržet pouze podniky operátorů, které se nacházejí ve Spojeném království, ačkoli definice komunikačního operátora uvedená v čl. 261 odst. 10 zákona IPA 2016 stanoví, že „telekomunikační operátor je osoba, která nabízí nebo poskytuje telekomunikační služby osobám ve Spojeném království nebo *osoba, která spravuje či provozuje telekomunikační systém, který se (zcela nebo částečně) nachází ve Spojeném království nebo je z něj spravován*“. Důsledkem toho by totiž osobní údaje subjektů údajů z EHP mohly být dotčeny, například kdyby shromážděné nebo vygenerované údaje podnik britského telekomunikačního operátora, který se nachází v EHP, předal na základě rozhodnutí o odpovídající ochraně (pro obchodní účely) podniku téhož operátora, který se nachází ve Spojeném království, a poté by tyto údaje byly shromážděny příslušným orgánem veřejné moci ve Spojeném království.

159. **EDPB je tudíž toho názoru, že posouzení těchto ustanovení je rovněž důležité pro posouzení odpovídající úrovně právního rámce Spojeného království a vyzývá Evropskou komisi, aby toto hledisko objasnila a dále posoudila, do jaké míry tomu tak je. EDPB především vyzývá Evropskou komisi, aby objasnila své porozumění rozsahu těchto právních předpisů, včetně představy o tom, co spadá do pojmu „uživatelé telekomunikačních služeb“, a zda by údaje podniků telekomunikačních operátorů mimo Spojené království, ve smyslu dotčených údajů subjektů údajů z EHP, mohly být vzhledem k velmi obecné definici telekomunikačních operátorů vyžádány.**

160. **Třetí bod** se týká postupu dvojité pojistky. EDPB uvádí, že nový postup dvojité pojistky byl zaveden v zákoně IPA 2016. EDPB rovněž uvádí, že i kdyby se teoreticky shromažďování údajů nebo přístup k údajům pro účely národní bezpečnosti či zpravodajství prováděl pouze na základě příkazu, který schválí soudní komisař, zákon IPA 2016 stanoví, že „*v omezených zvláštních případech je povoleno zákonné zachycování údajů bez příkazu, pouze na základě předchozího povolení samotných příslušných orgánů IC [viz oddíl níže týkající se dohledu], a to včetně zachycování údajů v souladu s mezinárodními žádostmi (článek 52 zákona IPA 2016)*“. Jak je uvedeno dále, toto rovněž potvrzuje obavy EDPB především v oblasti zahraničního zveřejňování. EDPB rovněž uvádí, že v případě vytěžování počítačové sítě, ať už cíleného, nebo hromadného, je možné využít odchylku od postupu dvojité pojistky a že soudní komisař je oprávněn povolit pouze obnovení hromadných příkazů po uplynutí maximální počáteční lhůty šesti měsíců. **EDPB vyzývá Evropskou komisi, aby dále posoudila a prokázala, že právní rámec Spojeného království poskytuje vhodné záruky i v případech, kdy neplatí postup dvojité pojistky, včetně záruk účinného dohledu *ex post* a dostupných opravných prostředků, aby byla zajištěna úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany poskytnuté v EU (viz také oddíl 4.3.3 níže týkající se dohledu).**

161. Ačkoliv zákon IPA 2016 skutečně zavedl postup dvojité pojistky, EDPB je stále znepokojen některými prvky v nových právních předpisech. Na základě uspořádání odpovídajících oddílů v návrhu rozhodnutí provedl EDPB analýzu následujících typů shromažďování údajů a přístupu k údajům v tomtéž pořadí, jaké uvedla Evropská komise. Pořadí následně posuzovaných prvků však neodpovídá prioritám podle úrovně znepokojení EDPB.

#### 4.3.1.2 Cílené získávání a uchovávání komunikačních údajů

162. EDPB uvádí, že existují dvě úřední osoby, které mohou udělovat povolení k cílenému získávání komunikačních údajů: schvalující úředník Úřadu pro schvalování komunikačních údajů (Office for Communications Data Authorisations) (dále jen „úředník IPC“) a pověřený vyšší úředník (osoba, která

[98] Viz 196. bod odůvodnění návrhu rozhodnutí.

zastává přidělený úřad nebo funkci v příslušném orgánu veřejné moci), nad rámec povolení soudního komisaře v určitých případech. EDPB však stále není jasné, který komisař povoluje podle právních předpisů a příslušného kodexu jaký druh cíleného získávání komunikačních údajů a do jaké míry by byl pověřený úředník dostatečně nezávislý[99].

163. **EDPB tudíž vyzývá Evropskou komisi, aby dále toto hledisko posoudila a poskytla k těmto prvkům jasnější vysvětlení.**

164. Pokud jde o oznámení, jimiž se žádá o uchovávání komunikačních údajů, EDPB uvádí, že taková oznámení mohou být určena i „popisu operátorů". Tento pojem zřejmě znamená, že uchovávání údajů může být požadováno po několika operátorech zároveň. Cílenost získávání údajů se ve skutečnosti nevztahuje na počet operátorů, ale na jméno nebo popis osob, organizací, místa nebo skupin osob, které představují „cílovou skupinu", popis povahy vyšetřování a popis činností, pro něž je zařízení používáno. EDPB tedy zdůrazňuje, že v závislosti na počtu operátorů, kterých se tento „popis operátorů" týká, může být oznámení obecnější, než se z postupu pro cílené uchovávání může zdát. **EDPB vyzývá Evropskou komisi, aby dále toto hledisko posoudila a poskytla další ujištění o tom, že i když budou oznámení určena několika operátorům, zůstanou omezena na to, co je bezpodmínečně nutné a přiměřené.**

#### 4.3.1.3 Vytěžování počítačové sítě

165. EDPB uvádí, že se „vytěžování počítačové sítě" může od postupu dvojité pojistky odchýlit v případě naléhavé potřeby[100]. EDPB se tudíž obává, že účely, pro něž může být takové vytěžování počítačové sítě požadováno, jsou obecné, a že kritéria naléhavé potřeby (kdy se po soudním komisaři nevyžaduje povolení *ex ante* pro posouzení nezbytnosti a přiměřenosti vytěžování počítačové sítě) zůstávají nejasná. Jelikož v takovém případě platí, že „příkaz pozbývá platnosti a nemůže být obnoven", pokud soudní komisař neschválí vytěžování počítačové sítě dodatečně, EDPB má za to, že údaje, které byly shromážděny mezitím, zůstávají shromážděny zákonným způsobem. Pro vymazání těchto údajů může být vydán zvláštní příkaz soudního komisaře[101].

166. **EDPB vyzývá Evropskou komisi, aby dále posoudila podmínky, podle kterých se lze odvolat na naléhavou potřebu, a objasnila možnosti výkonu práv dotčených subjektů údajů a možné opravné prostředky, které mají k dispozici v souvislosti s vytěžováním počítačové sítě k získávání údajů, zejména v případě odchylky od postupu dvojité pojistky.**

#### 4.3.1.4 Hromadné zachycování údajů od doručitelů

167. Jak se popisuje ve zprávě o přezkumu hromadných pravomocí[102] *„[h]romadné zachycování údajů zpravidla obnáší shromažďování komunikace na cestě mezi konkrétními doručiteli (komunikační spojení)*". Oficiální informativní přehled IPA 2016 popisuje „hromadné zachycování" jako„ *postup shromažďování objemu komunikace následovaný výběrem určité komunikace, kdy je nutné a přiměřené provést její přečtení, posouzení nebo odposlech*". EDPB uvádí, že „hromadné zachycování" údajů ve skutečnosti znamená shromažďování údajů ještě před jejich filtrováním selektory (buď jednoduše v rámci sledování známých osob, které představují hrozbu, nebo složitěji při určování nových hrozeb a dříve neznámých osob, které jsou předmětem zájmu).

[99] Viz také část níže věnovaná posouzení postupu dvojité pojistky a nezávislosti soudního komisaře.
[100] Viz článek 109 zákona IPA 2016.
[101] Viz čl. 110 odst. 3 písm. b) zákona IPA 2016.
[102] Viz zpráva „Report of the Bulk Powers Review" vypracovaná nezávislou osobou pro kontrolu právních předpisů v oblasti terorismu, srpen 2016.

168. Získávání hromadných komunikačních údajů bylo jedním z hlavních témat, která SDEU zkoumal v případě Privacy International, jehož výsledkem byl rozsudek velkého senátu vydaný 6. října 2020 (nad rámec posouzení, zda takové shromažďování údajů bylo provedeno v oblasti práva Unie, a to i pro účely národní bezpečnosti). Zákon IPA 2016 nahradil právní předpisy, které byly předmětem tohoto rozsudku.

169. EDPB uvádí, že díky zavedení zákona IPA 2016 do právního řádu Spojeného království se nyní vyžaduje příkaz také pro hromadné zachycování údajů. Postup pro vydání tohoto příkazu se spoléhá na vymezení „operativních účelů". Seznam těchto operativních účelů sestavují vedoucí zpravodajských služeb a poté jej schvaluje státní tajemník(-ice). Samotné rozhodnutí je schvalováno nezávislým soudním komisařem, který musí posoudit, zda je příkaz nezbytný a přiměřený pro operativní účely. EDPB chápe, že soudní komisař nemá pravomoc k posouzení samotných operativních účelů, nýbrž posuzuje, zda je příkaz nezbytný a přiměřený pro operativní účely, které uvádí. Kopie tohoto seznamu se každé tři měsíce předkládá Zpravodajskému a bezpečnostnímu výboru parlamentu a předseda vlády tento seznam operativních účelů alespoň jednou ročně přezkoumává.

170. Na základě prvků, které Evropská komise uvedla v návrhu rozhodnutí, se však zdá obtížné posoudit rozsah těchto operativních účelů uvedených na seznamu a také to, zda shromažďování údajů, které tyto účely umožňují, splňuje hranici stanovenou SDEU (například vymezení zeměpisné oblasti pro shromažďování údajů by mohlo zahrnovat několik ulic, nebo naopak celý EHP).

171. EDPB zdůrazňuje, že hromadně shromážděné údaje mohou být uchovávány na delší dobu (pro případ jejich dostupnosti pro další kontrolu). EPDB uvádí, že čl. 150 odst. 5 a 6 zákona IPA 2016 stanoví pouze zničení kopií shromážděných údajů, a to pouze pokud jejich uchovávání není nezbytné, případně pravděpodobně nebude nezbytné, v zájmu národní bezpečnosti nebo pro jiné důvody spadající do působnosti čl. 138 odst. 2 zákona IPA 2016, nebo pokud uchovávání údajů není nezbytné pro několik dalších účelů[103]. EDPB zdůrazňuje, že se tyto důvody jeví jako velmi obecné a v každém případě zmiňují pouze kopie získaných údajů.

172. Kromě toho EDPB dále uvádí, že v naléhavých případech zákon IPA 2016 rovněž umožňuje změnu příkazů bez předchozího schválení soudního komisaře. Pokud v takovém případě soudní komisař následně do tří pracovních dnů po změně příkazu odmítne tuto změnu schválit, bude mít příkaz účinnost, jako by se taková úprava neuskutečnila, ale údaje, které byly mezitím shromážděny, však zůstanou údaji shromážděnými zákonným způsobem[104]. Pro vymazání těchto údajů může být vydán zvláštní příkaz soudního komisaře[105].

173. **EDPB tudíž vyzývá Evropskou komisi, aby dále vysvětlila a posoudila hromadné zachycování údajů, zejména s ohledem na výběr a použití selektorů v rámci těchto postupů pro hromadné zachycování údajů, aby bylo objasněno, do jaké míry přístup k osobním údajům splňuje hranici určenou SDEU (viz oddíl 4.3.1.7 níže týkající se dohledu nad selektory), a jaké záruky jsou zavedeny na ochranu základních práv fyzických osob, jejichž údaje jsou v tomto ohledu zachycovány, včetně lhůt pro uchovávání údajů. Zvláště užitečné by bylo nezávislé posouzení, které by provedly příslušné orgány dohledu ve Spojeném království.**

[103] Viz čl. 150 odst. 3 a 6 zákona IPA 2016.
[104] Viz článek 147 zákona IPA 2016 (část 6, kapitola I).
[105] Viz čl. 181 odst. 3 písm. b) zákona IPA 2016.

174. **EDPB rovněž zdůrazňuje, že situace je o to závažnější, že „přeshraniční komunikace“, na kterou se vztahují praktiky hromadného zachycování údajů, zdánlivě umožňuje, aby údaje z EHP byly přímo zachycovány a hromadně shromažďovány Spojeným královstvím, a to včetně údajů na cestě mezi EHP a Spojeným královstvím, na něž by se vztahoval návrh rozhodnutí (viz oddíl 4.3.2 níže týkající se dalšího použití údajů shromážděných pro účely národní bezpečnosti a zahraničního zveřejňování).**

#### 4.3.1.5 Ochrana a záruky pro sekundární údaje

175. EDPB se obává, že příslušné právní předpisy Spojeného království, které se týkají hromadného zachycování údajů, neposkytují stejnou úroveň ochrany pro všechny komunikační údaje. „Sekundárními údaji“, které lze získat hromadným příkazem, jsou podle článku 137 zákona IPA 2016 jak „systémové údaje“, „*které jsou obsaženy, součástí, připojeny nebo logicky provázány s komunikací (odesilatelem nebo jinak)*“, tak „identifikační údaje“, „*které jsou obsaženy, součástí, připojeny nebo logicky provázány s komunikací (odesilatelem nebo jinak), jež lze logicky vyjmout ze zbytku komunikace, aniž by prozradily něco, co by mohlo být důvodně považováno za (případný) význam komunikace, bez ohledu na jakýkoli význam vyplývající z podstaty komunikace nebo některého z údajů, který se týká přenosu komunikace*“[106].

176. EDPB uvádí, že tyto hromadně shromažďované „sekundární údaje“, též známé jako „metadata“[107], zdánlivě nepožívají stejných záruk jako údaje shromažďované na základě cíleného příkazu, ale ani jako obsahové údaje shromažďované hromadně. EDPB si všímá, že výběr jakéhokoliv zachyceného obsahu skutečně požívá většího ochranného opatření[108] než výběr sekundárních údajů[109].

177. Kromě toho EDPB zdůrazňuje, že jak ESLP[110], tak SDEU[111] zpochybnily skutečnost, že takové údaje jsou méně citlivé než ostatní, zejména než obsahové údaje. Kodex zásad pro zachycování údajů uvádí příklady „sekundárních údajů“ (jak „systémových údajů“ jako nastavení routeru, e-mailové adresy, ID uživatelů a jiné identifikátory účtů, tak „identifikačních údajů“ jako místo konání schůzky podle

---

[106] „Systémové údaje“ a „identifikační údaje“ jsou definovány v článku 263 zákona IPA 2016.

[107] Viz zpráva „Report of the Bulk Powers Review“ vypracovaná nezávislou osobou pro kontrolu právních předpisů v oblasti terorismu, srpen 2016.

[108] Viz čl. 152 odst. 1 písm. c) a odst. 3 a následující zákona IPA 2016.

[108] Viz čl. 152 odst. 1 písm. c) a odst. 3 a následující zákona IPA 2016.

[109] Viz čl. 152 odst. 1) písm. a) a b) zákona IPA 2016.

[110] Viz rozsudek ESLP, Big Brother Watch, bod 357, postoupeno velkému senátu: „*Ačkoli tedy Soudní dvůr nepochybuje o tom, že komunikační údaje jsou zásadním nástrojem zpravodajských služeb v boji proti terorismu a závažné trestné činnosti, nedomnívá se, že orgány nastolily spravedlivou rovnováhu mezi veřejným a soukromým zájmem tím, že je zcela vyjmuly z ochranných opatření, která se vztahují na vyhledávání a zkoumání obsahu. Soudní dvůr nenaznačuje, že by související komunikační údaje měly být zpřístupněny pouze pro účely zjištění, zda se daná osoba nachází na Britských ostrovech, což by vyžadovalo uplatnění přísnějších kritérií na související komunikační údaje, než jaká se uplatňují na obsah, má však za to, že by měly být zavedeny dostatečné záruky, které zajistí, aby vyjmutí souvisejících komunikačních údajů z požadavků článku 16 zákona RIPA bylo omezeno do té míry, jež je nezbytná k určení, zda se osoba v danou chvíli nachází na Britských ostrovech.*“

[111] Viz rozsudek SDEU, Privacy International, bod 71: „*Zásah do práva zakotveného v článku 7 Listiny EU, který je způsoben předáváním dopravních a polohových údajů bezpečnostním a zpravodajským agenturám, musí být považován za obzvláště závažný, mimo jiné vzhledem k citlivé povaze informací, které tyto údaje v sobě nesou, a zejména vzhledem k možnosti sestavit profil dotyčných osob na základě těchto údajů, přičemž taková informace není o nic méně citlivá než samotný obsah komunikace. Zároveň to u dotčených osob pravděpodobně vyvolá pocit, že jejich soukromý život je pod neustálým dohledem (viz obdobně rozsudky ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238, body 27 a 37, a ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 99 a 100).*“

kalendáře, informace o fotografiích, např. čas, datum a místo, kde byly pořízeny). **EDPB tedy zdůrazňuje důsledné posuzování ze strany soudů ESLP a SDEU a připomíná obavy ohledně sekundárních údajů, které by z důvodu své citlivosti měly požívat výhod zvláštního ochranného opatření. EDPB proto vyzývá Evropskou komisi, aby důkladně posoudila, zda záruky stanovené v právních předpisech Spojeného království pro tuto kategorii osobních údajů zajišťují v zásadě rovnocennou úroveň ochrany jako v EU.**

#### 4.3.1.6 Automatizované zpracování komunikačních údajů

178. EDPB uvádí, že podle zprávy Zpravodajského a bezpečnostního výboru z roku 2015 orgány zpravodajské komunity nepoužívají k filtrování hromadně shromážděných údajů pouze jednoduché nebo složité selektory, ale mohou se rovněž spoléhat na nástroje automatizovaného zpracování pro analýzu *„velkého množství informací, které agenturám umožňuje hledat spojitosti, vzory, vztahy nebo chování, jež mohou odhalit vážnou hrozbu vyžadující prošetření“*[112]. **EDPB si je vědom skutečnosti, že se v této veřejné zprávě uvádějí postupy podle předchozího právního rámce, který byly následně nahrazeny zákonem IPA 2016. Domnívá se však, že je nutné provést další nezávislé posouzení a dohlížet nad používáním automatizovaných nástrojů pro zpracování ze strany příslušných orgánů dohledu ve Spojeném království, a vyzývá Evropskou komisi, aby dále tuto oblast posoudila, a to včetně záruk, které by v této souvislosti byly poskytovány, nebo mohly být poskytovány, subjektům údajů EHP.**

#### 4.3.1.7 Rizika nedodržování předpisů a nevyhovující postupy příslušných orgánů zpravodajské komunity

179. EDPB uvádí, že existují podrobné zprávy o dohledu. Tyto zprávy obsahují cenné informace o tom, jaké postupy se považují za vyhovující, ale také rizika nedodržování předpisů a nevyhovující postupy.

180. Podle zprávy komisaře IPC z roku 2019 v tomto ohledu několik informací o uplatňování právního rámce různými příslušnými orgány odhalilo (rizika) nedodržování předpisů těmito orgány.

181. Za prvé, EDPB si všiml, že kritéria pro klasifikaci souboru údajů jako hromadného souboru osobních údajů nebo cílených údajů se nezdají být vždy jasná ani samotným agenturám MI5 a SIS, zvláštně pak agentuře MI5, což může vést k tomu, že pro tyto údaje chybějí vhodné ochranné prostředky[113]. Ve své zprávě z roku 2019 komisař IPC doporučil, aby *„tato věc byla řešena jako priorita“*[114]. Za druhé si v této souvislosti EDPB všímá, že u britské zpravodajské služby GCHQ – ačkoli se klasifikace hromadných souborů osobních údajů jeví jako vyhovující (avšak ještě musí být podrobena auditu

[112] Viz dokument Zpravodajského a bezpečnostního výboru parlamentu, „Privacy and Security: A modern and transparent legal framework“, 2015, bod 18, s. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

[113] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019“, 15. prosince 2020, bod 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: *„Pozorujeme pozitivní vývoj [panelu hromadného dohledu (BOP)] a zaznamenáváme jeho dopad na řízení interního dodržování předpisů. Nadále usilujeme o lepší vyjasnění postupu, který používá agentura MI5 při úvodní kontrole nových souborů údajů, abychom lépe porozuměli rozhodnutí klasifikovat soubory údajů jako hromadné komunikační údaje nebo například cílené údaje. Znepokojil nás jeden nevyřešený bod v zápisu BOP týkající se řešení nesrovnalostí v případě rozdělení hromadných komunikačních údajů mezi agentury MI5 a SIS. Je možné, že z důvodu různého druhu použití údajů a různého množství uchovávaných údajů, mohly obě agentury uchovávat stejný soubor údajů nebo jeho verze, který jedna agentura mohla zákonným způsobem považovat za hromadné údaje a druhá za cílené údaje. Existuje riziko, že pokud jedna z agentur nesprávně klasifikovala uchovávané údaje jako cílené, byly by tyto údaje uchovávány bez příslušného příkazu a jako takové by nepodléhaly vhodným ochranným opatřením.“*

[114] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019“, bod 8.39.

komisaře IPC) – vzbudil v březnu 2019 vážné obavy interní přezkum dodržování požadavků v případě příkazů, který provedl specializovaný tým, jelikož 50 % odůvodnění pro vydání příkazů k hromadnému získávání údajů, které tým zpravodajské služby GCHQ přezkoumal, nesplňovalo požadovaný standard. Podle komisaře IPC zahájil tým pro dodržování předpisů šetření tohoto problému a rekvalifikoval zaměstnance, aby byl tento standard lépe dodržován. Obnovená školení zaměřená na ustanovení zákona IPA 2016 a další školení, která byla uspořádána v rámci politické sítě a sítě pro soulad s předpisy, pomohla zpravodajské službě GCHQ zlepšit dodržování předpisů v této oblasti. Komisař IPC neočekává, že by se v rámci budoucích kontrol tento standard snížil, nicméně bude nadále tuto oblast pozorně sledovat[115]. **Podle EDPB je tudíž nezbytné, aby Evropská komise provedla další přezkum a sledování uvedených skutečností v rámci posouzení úrovně ochrany s cílem ujistit se, že bylo dosaženo zlepšení tohoto standardu, jak zdůrazňuje zpráva komisaře IPC, a připomíná, že by při posuzování základní rovnocennosti třetí země rovněž mělo být zohledněno provádění a konkrétní uplatňování právního rámce, jak stanoví článek 45 GDPR.**

182. Obecně EDPB upozorňuje na body, jimž je třeba věnovat pozornost a které sdílel komisař IPC, zejména „úkolová-prohledávání" prováděná pracovníky MI5, která vyšetřovatelům umožňují provádět vícero prohledávání dostupných hromadných osobních údajů, a „*závažná rizika nedodržování předpisů související s některými technologickými prostředími, která jsou v agentuře MI5 využívána*", například, kde v daném prostředí byly údaje uloženy, kdo k nim měl přístup, v jaké míře byly kopírovány nebo sdíleny, platné postupy pro jejich vymazávání, jakož i lhůty pro jejich uchovávání. Ačkoliv komisař IPC uvádí, že byla přijata opatření a byly zavedeny záruky – některé z nich stále manuální, založené na individuálních lidských zdrojích – zdůrazňuje, že je rozhodující, že „*MI5 pokračuje v udržování těchto postupů a vynakládá dostatečné zdroje, aby mohly fungovat účinným způsobem. Pokud MI5 zpozoruje nárůst nevyhovujícího chování*"[116], komisař IPC očekává, že na něj bude bez prodlení upozorněn. **EDPB tudíž vyzývá Evropskou komisi, aby v budoucnu podrobně tyto aspekty sledovala**.

183. Pokud jde o zpravodajskou službu GCHQ, EDPB ze zprávy komisaře IPC chápe, že u operací prováděných na základě hromadných příkazů byla „*kvalita žádostí o interní schválení proměnlivá a zaznamenali jsme prostor pro zlepšení ve způsobu jejich formulace*"[117] a že u cíleného vytěžování počítačové sítě byla vysvětlení pro použití obecných deskriptorů někdy příliš obecná a nepřesná[118]. EDPB si rovněž povšiml, že v případě hromadného vytěžování počítačové sítě komisař IPC doporučuje, že „*žádosti by měly důsledně a výslovně zaznamenávat souvislost mezi cíleným a zákonným účelem a zpravodajskými požadavky*"[119], že „*všechny žádosti by měly jasně uvádět potenciál pro další narušení a příslušné zmírňování dopadů při posuzování proporcionality*"[120], a navzdory pokroku komisař IPC zdůraznil, že je „*stále prostor pro zlepšení*"[121] a v budoucnu bude zapotřebí tomuto věnovat další pozornost.

184. V souvislosti s režimem hromadného zachycování údajů podle nařízení o vyšetřovacích pravomocích z roku 2000 (RIPA), které již bylo nahrazeno ustanoveními zákona IPA 2016, EDPB připomíná, že nedostatečný dohled, jak nad výběrem internetových doručitelů pro zachycování, tak nad filtrováním, vyhledáváním a výběrem zachycované komunikace pro účely kontroly, byl jedním z

[115] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019", bod 10.48.
[116] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019", bod 8.52.
[117] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019", bod 10.2.
[118] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019", body 10.16 a 10.17.
[119] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019", bod 10.23.
[120] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019", bod 10.23.
[121] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019", bod 10.23.

hlavních aspektů, jenž podle ESLP nebyl v souladu s článkem 8 EÚLP s ohledem na dřívější právní předpisy týkající se vyšetřovacích pravomocí orgánů Spojeného království v oblasti národní bezpečnosti ve věci Big Brother Watch, která byl postoupena velkému senátu. **EDPB vyzývá Evropskou komisi, aby ověřila aktuální stav tohoto řízení, zohlednila veškeré informace v této věci a uvedla je ve svém rozhodnutí o odpovídající ochraně, pokud by jej Evropská komise přijala.**

185. V tomto případě ESLP: *„Není přesvědčen, že jsou bezpečnostní opatření, jimiž se řídí výběr doručitelů pro zachycování údajů a výběr zachycovaného materiálu pro kontrolu, dostatečně silná, aby poskytovala vhodné záruky proti zneužití. Nejvíce znepokojující je ovšem skutečnost, že chybí stabilní nezávislý dohled nad selektory a vyhledávacími kritérii, které se používají k filtrování zachytávané komunikace.“*[122] Jak zdůraznil komisař IPC, *„toto zjištění se odráží v doporučení dokumentu Zpravodajského a bezpečnostního výboru ‚Privacy and Security: A modern and transparent legal framework report‘ z března 2015“*[123]. **EDPB oceňuje, že komisař IPC následně provedl přezkum svého přístupu k hromadnému zachycování údajů v roce 2019, *„který zahrnoval pečlivý přezkum technicky složitých způsobů, v rámci nichž je hromadné zachycování skutečně prováděno“*,[124] a zavázal se od roku 2020 provádět při kontrolách hromadného zachycování údajů *„podrobné posuzování selektorů a vyhledávacích kritérií, na něž ve výše uvedené souvislosti poukázal ESLP“*[125]. Vzhledem k významu tohoto aspektu se EDPB obává, že důkladné posouzení selektorů a vyhledávacích kritérií ještě nebylo komisařem IPC provedeno a vyzývá Evropskou komisi, aby podrobně sledovala vývoj v této oblasti, zejména z toho důvodu, že konkrétní formát takového dohledu je stále nutné objasnit[126].**

### 4.3.2 Další použití údajů shromažďovaných pro účely národní bezpečnosti a zahraniční zveřejňování

186. Pokud jde o další použití údajů shromažďovaných pro účely národní bezpečnosti, Evropská komise ve svém hodnocení odkazuje na čl. 87 odst. 1 zákona DPA 2018, který stanoví, že *„takto shromážděné osobní údaje nesmějí být zpracovány způsobem, který se neslučuje s účelem, pro nějž byly shromážděny“*. EDPB ovšem upozorňuje, že toto ustanovení může podléhat výjimkám z důvodu národní bezpečnosti podle článku 110 zákona DPA 2018. EDPB dále uvádí, že právní předpisy stanoví možnost „zahraničního zveřejňování“, ať už v případě cíleného zachycování a kontroly, cíleného získávání a uchovávání komunikačních údajů, cíleného vytěžování počítačové sítě, nebo hromadného zachycování a hromadného vytěžování počítačové sítě.

#### 4.3.2.1 Další použití, zahraniční zveřejňování a platný právní rámec ve Spojeném království

187. Evropská komise označila část 4 zákona DPA 2018 a konkrétně její článek 109 jako důležitá ustanovení, která stanovují konkrétní požadavky na další použití shromážděných údajů a zejména zahraniční předávání osobních údajů zpravodajskými službami do třetích zemí nebo mezinárodním organizacím. EDPB ovšem uvádí, že článek 110 zákona DPA 2018 stanoví výjimku z důvodu národní bezpečnosti a uvádí, že některá ustanovení zákona DPA 2018 neplatí, pokud je výjimka z těchto ustanovení požadována pro účely zajištění národní bezpečnosti. Dotčená ustanovení, která nemusí být uplatněna, zahrnují část 4 kapitolu 2 zákona DPA 2018 týkající se zásad pro ochranu údajů, včetně

[122] Viz rozsudek ESLP, Big Brother Watch, bod 347.
[123] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019“, bod 10.28.
[124] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019“, bod 10.28.
[125] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019“, bod 10.28.
[126] Viz výroční zpráva „Annual Report of the Investigatory Powers Commissioner 2019“, bod 10.28: „přesný formát této kontroly ještě nebyl odsouhlasen“.

účelového omezení, jakož i část 4 kapitolu 3 zákona DPA 2018 týkající se práv subjektů údajů. Článek 109 zákona DPA 2018 ve spojení s článkem 110 zákona DPA 2018 a podmínkami, podle kterých platí, mohou vést k případům, kdy se zahraniční předání osobních údajů zpravodajskými službami do třetích zemí uskuteční bez použití ustanovení, která se vztahují na zásady pro ochranu údajů a práva subjektů údajů.

188. Jak určila Evropská komise, taková výjimka se musí posoudit na základě konkrétního případu a lze ji uplatnit, pouze pokud by konkrétní ustanovení mělo negativní důsledky pro národní bezpečnost. Cílem vydání vnitrostátního osvědčení pro zpravodajské služby Spojeného království je skutečně potvrdit, že výjimka je požadována pro konkrétní osobní údaje, které jsou zpracovávány pro účely zajištění národní bezpečnosti. EDPB však uvádí, že ministerstvo vnitra Spojeného království ve svých pokynech k národnímu bezpečnostnímu osvědčení podle zákona DPA 2018 upřesňuje, že *„[j]e důležité na začátku zmínit, že osvědčení není pro uplatnění výjimky z důvodu národní bezpečnosti nutné; ve většině případů si dokonce správci sami určí, zda je výjimka z důvodu národní bezpečnosti použitelná*“.[127] Kromě toho se v pokynech ministerstva vnitra Spojeného království uvádí, že *„národní bezpečnostní osvědčení mohou platit pro osobní údaje, které se dají konkrétně určit, nebo které zahrnují obecnější kategorii osobních údajů. Mohou být předběžná i se zpětnou účinností*“.[128] Výjimka z důvodu národní bezpečnosti se tudíž může uplatnit na zahraniční předávání osobních údajů zpravodajskými službami do třetích zemí i bez národního bezpečnostního osvědčení.

189. EDPB dále uvádí, že například národní bezpečnostní osvědčení „DPA/S27/Security Service“[129] stanoví, že osobní údaje zpracovávané *„pro, Britské bezpečnostní služby, jejich jménem, na jejich žádost nebo s jejich pomocí*“, a *„pokud je takové zpracování nezbytné k řádnému plnění úkolů Britské bezpečnostní služby, které jsou uvedeny v článku 1 zákona o bezpečnostních službách z roku 1989“* jsou do 24. července 2024 osvobozeny od ustanovení právního řádu Spojeného království, která odpovídají kapitole V GDPR o předávání osobních údajů do třetích zemí nebo mezinárodním organizacím. Ačkoli jiná veřejně dostupná národní bezpečnostní osvědčení neposkytují osvobození od ustanovení článku 109 zákona DPA 2018, je třeba připomenout, že částečné nebo úplné znění národního bezpečnostního osvědčení může být vyňato, pokud by jeho zveřejnění bylo v rozporu se zájmy národní bezpečnosti, s veřejným zájmem nebo by ohrozilo bezpečnost kterékoli osoby.

190. Při posuzování návrhu rozhodnutí v souvislosti s těmito ustanoveními si EDPB všiml, že se ochranná opatření pro taková zveřejnění skládají výhradně z požadavku, aby příjemce údajů respektoval podmínky, které se týkají bezpečnosti údajů, nezbytně nutné míry pro zveřejnění, uchovávání údajů a omezení přístupu k údajům pro nezbytný počet osob. **EDPB** tedy **zdůrazňuje, že v případě zahraničního zveřejňování údajů může použití výjimky z důvodu národní bezpečnosti, která je stanovena v právním řádu Spojeného království, vést k situacím, kdy by záruky zajišťující dodržování zásad účelového omezení, nezbytnosti a proporcionality, jakož i práva fyzických osob, dohled a opravné prostředky, nemusely být zcela zajištěny nebo respektovány ve třetí zemi určení. EDPB proto doporučuje, aby Evropská komise dále prozkoumala celkové záruky stanovené v právním řádu Spojeného království v případě zahraničního zveřejňování údajů, zejména pokud jde o použití výjimek z důvodu národní bezpečnosti.**

[127] Viz dokument ministerstva vnitra „The Data Protection Act 2018, National Security Certificates guidance“, srpen 2020, bod 3, s. 3.
[128] Viz dokument ministerstva vnitra „The Data Protection Act 2018, National Security Certificates guidance“, srpen 2020, bod 5, s. 4.
[129] Viz DPA/S27/Security Service, článek 27 zákona DPA 2018, Osvědčení státního tajemníka, 24. července 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

#### 4.3.2.2 Zahraniční zveřejňování a sdílení zpravodajských informací v rámci mezinárodní spolupráce

191. EDPB uvádí, že Evropská komise v rámci svého hodnocení nevzala v úvahu existující mezinárodní dohody uzavřené mezi Spojeným královstvím a třetími zeměmi nebo mezinárodními organizacemi, které mohou stanovit zvláštní ustanovení pro mezinárodní předávání osobních údajů zpravodajskými službami do třetích zemí.

192. EDPB rovněž zdůrazňuje, že se hodnocení Evropské komise soustředí převážně na posouzení části 4 zákona DPA 2018 a je obzvláště znepokojen, že se zákon IPA 2016 zaměřuje na „žádosti" o výměnu zpravodajských informací se zahraničními partnery, ale neuvádí jiné formy sdílení zpravodajských informací. V tomto ohledu EDPB uvádí, že se v návrhu rozhodnutí Evropské komise nezmiňuje ani neposuzuje propojení právního rámce Spojeného království s „dohodou mezi Spojeným královstvím a USA o zpravodajské komunikaci" (dále jen „dohoda UKUSA"). V nedávném prohlášení k 75. výročí této dohody americká Národní bezpečnostní agentura (NSA) uvedla, že toto partnerství umožňuje *„sdílet informace mezi oběma agenturami v co největší možné míře a s minimálními omezeními"* a že *„tento průlomový dokument vytvořil pro britské a americké zpravodajské odborníky politiku a postupy pro sdílení komunikace, překladů, analýz a dekódovacích informací"*.[130] Tato dohoda se stala základem pro vznik dalších partnerství v oblasti zpravodajství s Austrálií, Kanadou a Novým Zélandem.

193. Tajná povaha této dohody a její zvláštní ustanovení představují zásadní výzvu z hlediska jasnosti a předvídatelnosti právních předpisů v souvislosti s dalším používáním a zahraničním zveřejňováním údajů, které shromažďují orgány Spojeného království pro účely národní bezpečnosti. V tomto ohledu EDPB připomíná, že pokud jde o úroveň ochrany údajů zajišťovanou v EU, SDEU zdůraznil, že právní předpisy zasahující do základního práva na ochranu osobních údajů musí *„stanovit jasná a přesná pravidla pro rozsah a použití dotčeného opatření, která stanoví minimální požadavky, tak aby osoby, o jejichž osobní údaje se jedná, měly dostatečné záruky umožňující účinně chránit své údaje proti riziku zneužití a proti jakémukoli neoprávněnému přístupu k těmto údajům a jejich protiprávnímu využívání. Potřeba takových záruk je o to významnější v případě, kdy jsou osobní údaje zpracovávány automaticky, a existuje značné riziko neoprávněného přístupu k těmto údajům"*[131]. EDPB se tudíž domnívá, že by Evropská komise měla jako součást svého hodnocení o odpovídající úrovni posoudit dopad dohody UKUSA.

194. ESLP v první části svého rozsudku ze dne 13. září 2018 ve věci Big Brother Watch posoudil režim sdílení zpravodajských informací Spojeného království a zejména dohodu UKUSA. ESLP uvedl, že *„zákonný rámec, který zpravodajským službám Spojeného království povoluje požadovat zachycený materiál od zahraničních zpravodajských agentur, není uveden v zákoně RIPA. Dohoda mezi Spojeným královstvím a USA o zpravodajské komunikaci ze dne 5. března 1946 povoluje výměnu materiálu mezi Spojenými státy a Spojeným královstvím"*[132], a usoudil, že existuje *„právní základ pro vyžádání zpravodajských informací od zahraničních zpravodajských agentur a že uvedený právní předpis je dostatečně přístupný."*[133] Ačkoli ESLP shledal, že v souvislosti s režimem sdílení zpravodajských informací nedošlo k žádnému porušení článku 8 EÚLP[134], EDPB uvádí, že tento rozsudek byl nyní postoupen velkému senátu, na jehož rozhodnutí se stále čeká. EDPB rovněž uvádí, že v částečně

[130] Viz tisková zpráva agentury NSA „GCHQ and NSA Celebrate 75 Years of Partnership", 5. února 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.
[131] Viz Schrems I, bod 91.
[132] Viz rozsudek ESLP, Big Brother Watch, bod 425.
[133] Viz rozsudek ESLP, Big Brother Watch, bod 427.
[134] Viz rozsudek ESLP, Big Brother Watch, bod 448.

souhlasném, částečně nesouhlasném stanovisku k tomuto rozsudku soudkyně Koskelo společně se soudkyní Turković[135] dospěla k závěru, že k porušení článku 8 EÚLP v souvislosti s režimem sdílení zpravodajských informací došlo a uvedla, že *„[l]ze jednoduše souhlasit se zásadou, že by v rámci žádného ujednání, podle kterého jsou zpravodajské informace zachycené z komunikace prostřednictvím zahraničních zpravodajských služeb, ať už na základě žádostí o provedení takového zachytávání, nebo žádostí o sdělení jeho výsledků, nemělo být připuštěno obcházení záruk, které musí být pro jakékoli sledování vnitrostátními orgány zavedeny (viz body 216, 423 a 447). Jakýkoli jiný přístup by byl v podstatě nepřípustný*".

195. Jak dokládá několik zpráv ze sdělovacích prostředků a nevládních organizací[136] [137], poslední verze dohody UKUSA, která byla zveřejněna, pochází z roku 1956 a od té doby se komunikační technologie a signálové zpravodajství významně změnily. Zprávy sdělovacích prostředků například odhalily, že údaje přepravované podmořskými kabely, které dorazí do Spojeného království, jsou zachycovány zpravodajskou službou GCHQ a zpřístupňovány agentuře NSA[138].

196. Pro EDPB je klíčovou otázkou v oblasti sdílení zpravodajských informací, zda článek 109 zákona DPA 2018 a ustanovení zákona IPA 2016 zůstávají v platnosti, pokud zpravodajské služby Spojeného království budou jednat v souladu s dohodou UKUSA. Dalším klíčovým prvkem k posouzení je, zda ustanovení nebo účinné uplatnění této dohody má vliv na úroveň ochrany osobních údajů na cestě z EHP do Spojeného království nebo umožňuje jiným zpravodajským službám ve třetích zemích přímý přístup a získání osobních údajů.

197. Kromě výhrad, které EDPB vyjádřil ohledně „zahraničního zveřejňování" na základě části 4 zákona DPA 2018 a s tím souvisejících výjimek z důvodu národní bezpečnosti, jakož i žádostí v rámci zákona IPA 2016, **je v důsledku toho EDPB znepokojen používáním jiných forem sdílení a zveřejňování informací pomocí jiných nástrojů, především různých mezinárodních dohod, které Spojené království uzavřelo s jinými třetími zeměmi, zejména pokud takové nástroje zůstávají veřejnosti nepřípustné, například dohody UKUSA. Účinky takové dohody by mohly vést k obcházení stanovených záruk v oblasti přístupu k osobním údajům a jejich používání pro účely národní bezpečnosti.**

198. EDPB sdílí názor, který vyjádřil zvláštní zpravodaj OSN Joe Cannatacci, a to, že *„[s]dílení zpravodajských informací nesmí sloužit jako tajný způsob, jak získat nebo umožnit ostatním získávat zpravodajské informace osvobozené od domácích záruk, ani jako mezera v zákoně, která zahraničním vládám s nižší úrovní ochrany soukromí (nebo jiných lidských práv) umožní získávat zpravodajské informace od zpravodajských služeb Spojeného království, které by mohly vést k porušování lidských práv"*[139].

---

[135] Viz ESLP, Big Brother Watch, částečně souhlasné, částečně nesouhlasné stanovisko soudkyně Koskelo společně se soudkyní Turković.

[136] Viz článek BBC „Diary reveals birth of secret UK-US spy pact that grew into Five Eyes", 5. března 2021, https://www.bbc.com/news/uk-56284453.

[137] Viz zpráva Privacy International „Policy Briefing - UK Intelligence Sharing Arrangements", duben 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.

[138] Viz článek The Guardian „GCHQ taps fibre-optic cables for secret access to world's communications", 21. června 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[139] Viz vyjádření zvláštního zpravodaje „End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland", Londýn,

199. Kromě toho se **EDPB domnívá, že uzavírání dvoustranných a mnohostranných dohod se třetími zeměmi pro účely spolupráce zpravodajských služeb, které poskytnou právní základ pro přímé zachycování a získávání osobních údajů nebo pro předávání osobních údajů do třetích zemí, může rovněž významně ovlivnit podmínky dalšího používání shromážděných informací, jelikož tyto dohody pravděpodobně budou mít dopad na posuzovaný právní rámec Spojeného království pro ochranu údajů.**

### 4.3.3 Dozor

200. EDPB zdůrazňuje význam komplexního dohledu nezávislých dozorových úřadů pro zajištění vhodné úrovně ochrany údajů. Záruka nezávislosti dozorových úřadů ve smyslu čl. 8 odst. 3 Listiny EU má za úkol zajistit účinné a spolehlivé sledování dodržování pravidel pro ochranu osob v oblasti zpracování osobních údajů.

201. Jsou-li osobní údaje zpřístupněny a používány pro účely národní bezpečnosti, vykonává funkci dozoru především komisař IPC a soudní komisaři.

202. **EDPB obecně považuje zavedení soudních komisařů v zákoně IPA 2016 za výrazné zlepšení.** V souladu s výše uvedeným požadavkem se Evropská komise vyzývá, aby **podrobněji posoudila nezávislost soudních komisařů a především to, do jaké míry je nezávislost komisaře IPC a úřadu IPC (dále jen „IPCO“) zajištěna z právního hlediska, jelikož tato informace není uvedena v zákoně IPA 2016.** Ještě důležitější to je vzhledem k tomu, že komisař IPC rozhoduje v případě vládních odvolání, pokud bylo sledovací **opatření zamítnuto** soudním komisařem.

203. Komisař IPC má funkci dohledu *ex ante* i *ex post*. Pokud jde o dohled *ex ante*, EDPB má za to, že funkcí soudního komisaře je schválit v jednotlivých případech sledovací opatření, včetně cíleného zachycování a hromadného získávání komunikačních údajů. EDPB dále uvádí, že předchozí schválení sledovacích opatření nelze z judikatury SDEU odvodit jako absolutní požadavek na přiměřenost sledovacích opatření.[140]

204. Aby bylo možné posoudit účinnost této úrovně dohledu, EDPB považuje za nutné dále objasnit situace, v nichž je umožněno zákonné zachycování informací bez předchozího schválení soudních komisařů.

205. Ve svém návrhu rozhodnutí Evropská komise v poznámkách pod čarou č. 201 a č. 266 zmiňuje „zvláštní omezené případy“, které v souvislosti s cíleným zachycováním údajů stanoví zákon IPA 2016 v článcích 44 až 52. EDPB uvádí, že články 45 až 51 zákona IPA 2016 jsou výjimky, které zpravodajské služby údajně pravidelně nepoužívají. Kromě toho se **EDPB domnívá**, že v **případech, kdy se výjimky uplatňují** (např. poskytovatelé telekomunikačních a poštovních služeb), se předchozí schválení soudních komisařů provede, pokud orgány pro vymáhání práva nebo zpravodajské služby **požádají** o přístup k těmto údajům, a vyzývá **Evropskou komisi, aby ve svém rozhodnutí potvrdila, že tato domněnka je správná**.

206. EDPB uznává, že čl. 44 odst. 2 zákona IPA 2016 povoluje zachycování komunikace, pokud s tím jedna ze stran (odesílatel nebo příjemce) souhlasí a existuje-li oprávnění podle nařízení RIPA 2000 nebo

---

29. června 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] Rovněž uvádí, že SDEU při zrušení štítu na ochranu soukromí ve věci Schrems II, zohlednil skutečnost, že podle amerického právního řádu takzvaný soud FISA Court „*neschvaluje jednotlivá sledovací opatření; nýbrž schvaluje programy dozoru (jako PRISM, UPSTREAM) na základě ročních schválení*“ (bod 179).

nařízení k zákonu o vyšetřovacích pravomocích (Skotsko) z roku 2000 (2000 asp 11), tj. dřívější stav před zavedením soudních komisařů. EDPB **vyzývá** Evropskou komisi, aby objasnila, zda toto znamená, že by v případě jednostranného souhlasu nebylo předchozí schválení postupu vůbec vyžadováno.

207. Pokud jde o dohled *ex post*, je rovněž důležité ověřit, že je zajištěn bezproblémový a účinný nezávislý dohled, zejména pokud není zajištěn *ex ante*.

208. EDPB uvádí, že podle článků 48 až 52 zákona IPA 2016 soudní komisaři provádějí přezkum *ex post* a **vyzývá Evropskou komisi, aby objasnila, podle jakých požadavků a na čí žádost se takový přezkum *ex post* provádí**.

209. Podle čl. 229 odst. 4 zákona IPA 2016 komisař IPC nepřezkoumává výkon některých funkcí. V tomto ohledu EDPB vyzývá Evropskou komisi, aby objasnila ustanovení čl. 229 odst. 4 písm. d) a e) zákona IPA 2016 a jeho praktický dopad na způsobilost komisaře IPC k přezkumu. **EDPB má za to, že úřad ICO je příslušným dozorovým orgánem, na nějž se vztahuje výjimka z ustanovení čl. 229 odst. 4 zákona IPA 2016, a vyzývá Evropskou komisi, aby ve svém rozhodnutí potvrdila, že tato domněnka je správná.**

210. **Zdá se, že při provádění dohledu** *ex post* je úloha **komisaře IPC omezena** na vydávání doporučení v případech nedodržování předpisů a podávání oznámení subjektům údajů, pokud je chyba závažná a je ve veřejném zájmu, aby o tom osoba byla informována. **EDPB vyzývá Evropskou komisi, aby objasnila, jakým způsobem může úřad IPC zajistit účinné dodržování právních předpisů.**

211. **EDPB má za to, že dotčené osoby nemohou kontaktovat úřad IPCO přímo na jeho adrese, ale musí podat stížnost k úřadu IPCO, který má ovšem omezené kompetence v oblasti národní bezpečnosti. EDPB tedy vyzývá Evropskou komisi, aby dále objasnila, jak je z právního hlediska zajištěno, aby se úřad IPCO v takových případech stížnostmi zabýval.**

### 4.3.4 Náprava

212. Na základě rozsudků ve věci Schrems I a Schrems II je zřejmé, že účinná soudní ochrana ve smyslu článku 47 Listiny EU má zásadní význam pro předpoklad odpovídající úrovně právních předpisů ve třetí zemi. Tato usnesení rovněž prokázala, že zvláštní pozornost musí být v tomto ohledu věnována účinné soudní ochraně v oblasti přístupu k údajům pro účely národní bezpečnosti.

213. **EDPB oceňuje, že Spojené království založilo Tribunál IPT. Tribunál IPT má kompetenci rozhodovat ve věcech využití vyšetřovacích pravomocí nejen donucovacími orgány, ale i zpravodajskými službami. EDPB má za to, že Tribunál IPT funguje jako řádný soud ve smyslu článku 47 Listiny EU. Pokud jde o jeho pravomoci, Evropská komise se vyzývá, aby potvrdila, že Tribunál IPT má veškeré pravomoci uvedené v 262. bodě odůvodnění návrhu rozhodnutí, bez ohledu na právní základ, podle něhož je stížnost podávána.**

214. Utajené sledování zpravodajských služeb často znamená, že předmět sledování, tj. subjekt údajů, si není a nebude takového sledování vědom. V této souvislosti EDPB při své analýze amerického právního řádu mnohokrát vyjádřil své obavy ohledně požadavku „*locus standi*“, jak jej vykládá americký právní řád v případech sledování. V této souvislosti EDPB uvádí, že žaloba podaná k Tribunálu IPT vyžaduje pouze zkoušku z „přesvědčení“, podle níž žalobce musí dokázat, že mu hrozí potenciální riziko, že se na něj vztahuje opatření.

215. EDPB při analýze Tribunálu IPT věnuje zvláštní pozornost také tomu, že fungování Tribunálu IPT bylo opakovaně v souladu s EÚLP, tak jak ji vykládá ESLP.