

# Opinion of the Board (Art. 70.1.s)



**Stanovisko č. 5/2023 k návrhu prováděcího rozhodnutí  
Evropské komise o odpovídající ochraně osobních údajů  
podle rámce EU-USA pro ochranu údajů**

**Přijato dne 28. února 2023**

Dne 13. prosince 2022 zveřejnila Evropská komise návrh rozhodnutí o odpovídající ochraně (dále jen „návrh rozhodnutí“), který obsahuje přílohy představující nový rámec pro transatlantické výměny osobních údajů, tzv. rámec EU-USA pro ochranu údajů (dále jen „rámec pro ochranu údajů“), který má nahradit předchozí štít EU-USA na ochranu soukromí, který zrušil Soudní dvůr Evropské unie (dále jen „SDEU“) rozsudkem ze dne 16. července 2020 ve věci Schrems II. Klíčovou složkou rámce pro ochranu údajů jsou zásady rámce EU-USA pro ochranu údajů včetně doplňkových zásad (dále společně „zásady rámce pro ochranu údajů“).

V souladu s čl. 70 odst. 1 písm. s) nařízení Evropského parlamentu a Rady (EU) 2016/679<sup>1</sup> (dále jen „GDPR“) si Komise vyžádala stanovisko Evropského sboru pro ochranu údajů (dále jen „EDPB“) k návrhu rozhodnutí.

EDPB posoudil odpovídající úroveň ochrany poskytované v USA na základě posouzení návrhu rozhodnutí. EDPB posuzoval jak obchodní aspekty, tak přístup orgánů veřejné moci v USA k osobním údajům předávaným z EU a jejich využívání těmito orgány.

EDPB zohlednil platný právní rámec EU pro ochranu údajů stanovený v GDPR, jakož i základní práva na soukromý život a ochranu údajů zakotvená v článcích 7 a 8 Listiny základních práv Evropské unie a v článku 8 Evropské úmluvy o lidských právech. Zohlednil rovněž právo na účinnou právní ochranu a spravedlivý proces stanovené v článku 47 Listiny, jakož i v judikatuře týkající se jednotlivých základních práv.

EDPB navíc zohlednil i požadavky referenčního rámce pro odpovídající ochranu přijatého sborem EDPB<sup>2</sup>.

Hlavním cílem EDPB je poskytnout Evropské komisi stanovisko k odpovídající úrovni ochrany poskytované fyzickým osobám, jejichž osobní údaje jsou předávány do USA. Je důležité vzít na vědomí, že EDPB neočekává, že by právní rámec USA pro ochranu údajů replikoval evropské právo v oblasti ochrany údajů.

EDPB ovšem připomíná, že aby právní předpisy třetí země mohly být považovány za předpisy zajišťující odpovídající úroveň ochrany, musí podle požadavku článku 45 GDPR a judikatury SDEU zajišťovat subjektům údajů úroveň ochrany v zásadě rovnocennou úrovni ochrany zajištěné v EU.

### 1.1 Obecné aspekty ochrany údajů

Rámec pro ochranu údajů stanoví, že dodržování zásad rámce pro ochranu údajů organizacemi podle rámce pro ochranu údajů může být v některých případech omezeno (např. v rozsahu nezbytném pro splnění soudního příkazu nebo pro uspokojení veřejného zájmu). Aby bylo možné lépe určit dopad těchto výjimek na úroveň ochrany subjektů údajů, EDPB doporučuje, aby Komise do návrhu rozhodnutí zahrнула objasnění rozsahu těchto výjimek včetně platných záruk podle práva USA.

---

<sup>1</sup> 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 (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

<sup>2</sup> Pracovní skupina zřízená podle článku 29, Referenční rámec pro odpovídající ochranu, WP 254 rev. 01 ze dne 28. listopadu 2017, naposledy pozměněný a přijatý dne 6. února 2018 a schválený EDPB dne 25. května 2018 (dále jen „referenční rámec pro odpovídající ochranu“).

EDPB konstatuje, že vzhledem ke struktuře příloh a jejich číslování je poměrně obtížné tyto informace nalézt a odkazovat na ně. To přispívá k celkově složité prezentaci tohoto nového rámce, v jehož přílohách jsou shromážděny dokumenty různé právní hodnoty a který ne vždy napomáhá tomu, aby subjekty údajů, organizace podle rámce pro ochranu údajů a úřady EU pro ochranu údajů správně pochopily zásady rámce pro ochranu údajů. EDPB rovněž zdůrazňuje, že terminologie by měla být používána v celém rámci pro ochranu údajů jednotně. Stejně tak chybí definice některých základních pojmů<sup>3</sup>.

EDPB vítá aktualizace zásad rámce pro ochranu údajů<sup>4</sup>, které budou představovat závazný právní rámec pro organizace podle rámce pro ochranu údajů, konstatuje však, že navzdory řadě změn a dodatečných vysvětlení uvedených v bodech odůvodnění návrhu rozhodnutí zůstávají zásady rámce pro ochranu údajů, které musí organizace podle rámce pro ochranu údajů dodržovat, v podstatě beze změny s ohledem na zásady použitelné v rámci štítu EU-USA na ochranu soukromí (z nichž vychází každoroční společné přezkumy pracovní skupiny zřízené podle článku 29 a EDPB). Zásady rámce pro ochranu údajů jsou také do značné míry stejné jako zásady navrhovaného štítu na ochranu soukromí, na nichž pracovní skupina zřízená podle článku 29 založila své stanovisko z roku 2016<sup>5</sup>. U zásad rámce pro ochranu údajů, které se podstatně nezměnily, nepovažuje EDPB za nutné opakovat všechny připomínky, které již dříve vznesla pracovní skupina zřízená podle článku 29. EDPB se rozhodl zaměřit se na konkrétní aspekty, které dnes považuje za ještě relevantnější s ohledem na vývoj právního a technologického prostředí.

EDPB například konstatuje, že některé problémy, na které již dříve upozornila pracovní skupina zřízená podle článku 29 a EDPB ve vztahu k zásadám štítu na ochranu soukromí, přetrvávají i nadále. Týkají se zejména práv subjektů údajů (např. některých výjimek z práva na přístup a načasování a způsobů uplatnění práva vznést námitku), absence klíčových definic, nejasností ve vztahu k uplatňování zásad rámce pro ochranu údajů na zpracovatele a rozsáhlé výjimky pro veřejně dostupné informace<sup>6</sup>.

EDPB by rovněž rád zopakoval, že úroveň ochrany fyzických osob, jejichž údaje jsou předávány, nesmí být narušena dalším předáváním ze strany původního příjemce předávaných údajů<sup>7</sup>. EDPB znovu vyzývá Komisi, aby objasnila, že záruky uložené původním příjemcem dovozci ve třetí zemi musí být před dalším předáním v souvislosti s rámcem pro ochranu údajů účinné s ohledem na právní předpisy třetí země.

Obzvláštní pozornost vyžaduje rychlý vývoj v oblasti automatizovaného rozhodování a profilování – stále častěji pomocí technologií umělé inteligence. EDPB vítá odkazy Komise na konkrétní záruky, které poskytují příslušné právní předpisy USA v různých oblastech<sup>8</sup>. Zdá se však, že úroveň ochrany fyzických osob se liší podle toho, která odvětvová pravidla – pokud existují – se na danou situaci vztahují. EDPB trvá na tom, že k poskytnutí dostatečných záruk jsou zapotřebí zvláštní pravidla týkající se

---

<sup>3</sup> To se týká pojmů „zmocněnec“ a „zpracovatel“. Kromě toho je třeba s orgány USA ještě projednat pojem „údaje o lidských zdrojích“.

<sup>4</sup> Například objasnění, že údaje kódované pomocí klíče představují osobní údaje.

<sup>5</sup> Dokument pracovní skupiny zřízené podle článku 29, stanovisko č. 1/2016 k návrhu rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí, přijaté dne 13. dubna 2016 (dále jen „stanovisko skupiny WP 29 č. 1/2016“).

<sup>6</sup> Štít EU-USA na ochranu soukromí – třetí každoroční společný přezkum, zpráva EDPB přijatá dne 12. listopadu 2019, bod 11.

<sup>7</sup> Referenční rámec GDPR pro odpovídající ochranu, 3.A.9.

<sup>8</sup> Návrh rozhodnutí, 35. bod odůvodnění.

automatizovaného rozhodování, včetně práva fyzické osoby znát příslušnou logiku, práva napadnout rozhodnutí a práva na lidský zásah, pokud se jí rozhodnutí významně dotýká.

EDPB připomíná význam účinného dohledu a prosazování rámce pro ochranu údajů a domnívá se, že kontroly souladu mají zásadní význam, pokud jde o podstatnější požadavky. EDPB bude tyto aspekty úzce monitorovat, a to i v souvislosti s pravidelnými přezkumy. EDPB bere na vědomí obnovené závazky obsažené v dopisech Federální obchodní komise USA (Federal Trade Commission, dále též „FTC“)<sup>9</sup> a Ministerstva dopravy USA<sup>10</sup>, pokud jde o prosazování práva, např. upřednostnit vyšetřování údajných porušení rámce pro ochranu údajů.

EDPB konstatuje, že subjektům údajů z EU je poskytnuto sedm možností nápravy, pokud jsou jejich osobní údaje zpracovávány v rozporu s rámcem pro ochranu údajů. Tyto nápravné mechanismy jsou stejné jako mechanismy obsažené v bývalém štítu na ochranu soukromí, který byl předmětem připomínek pracovní skupiny zřízené podle článku 29<sup>11</sup>. EDPB bude úzce monitorovat účinnost těchto nápravných mechanismů, a to i v souvislosti s pravidelnými přezkumy.

## **1.2 Přístup k osobním údajům předávaným z Evropské unie a jejich použití orgány veřejné moci v USA**

V návrhu rozhodnutí dospěla Evropská komise k závěru, že „jakýkoli zásah do základních práv fyzických osob, jejichž osobní údaje jsou předávány z Unie do USA podle rámce EU-USA pro ochranu údajů, který je proveden ve veřejném zájmu, zejména pro účely prosazování trestního práva a pro účely národní bezpečnosti, ze strany orgánů veřejné moci USA bude omezen na to, co je nezbytně nutné k dosažení dotčeného legitimního cíle, a že existuje účinná právní ochrana proti takovému zásahu“<sup>12</sup>.

Evropská komise ke svému závěru dospěla po rozsáhlém posouzení prezidentského dekretu č. 14086 o posílení záruk pro činnosti signálového zpravodajství USA (dále jen „dekret EO 14086“). Dekret EO 14086 vydal prezident USA dne 7. října 2022 na základě jednání Evropské komise s vládou USA bezprostředně poté, co Soudní dvůr Evropské unie (SDEU) zrušil platnost předchozího rozhodnutí o odpovídající ochraně nazvaného „štít na ochranu soukromí“.

EDPB by uvítal, kdyby nejen vstup v platnost, ale i přijetí tohoto rozhodnutí byly podmíněny mimo jiné přijetím aktualizovaných politik a postupů k provádění dekretu EO 14086 všemi zpravodajskými službami USA. EDPB doporučuje Komisi, aby tyto aktualizované politiky a postupy posoudila a toto posouzení se sborem EDPB sdílela.

Pokud jde o přístup vlády k osobním údajům předávaným do USA, EDPB se ve své analýze zaměřil na posouzení nového dekretu EO 14086, neboť jeho faktickým účelem je řešit a napravit nedostatky, které SDEU identifikoval ve svém rozsudku ve věci Schrems II, když shledal předchozí rozhodnutí o odpovídající ochraně neplatným.

EDPB uznává, že právní rámec USA pro činnosti signálového zpravodajství byl pozměněn přijetím dekretu EO 14086, a považuje dodatečné záruky obsažené v tomto dekretu za významné zlepšení. Dekret EO 14086 zavádí do právního rámce USA pro signálové zpravodajství pojmy nezbytnosti a přiměřenosti a v případě, že by EU měla být označena za způsobilou organizaci regionální hospodářské integrace, poskytuje nový nápravný mechanismus pro fyzické osoby z EU. EDPB se domnívá, že tento nový nápravný mechanismus je ve srovnání s předchozím tzv. mechanismem ombudsmana v rámci

---

<sup>9</sup> Návrh rozhodnutí, příloha IV.

<sup>10</sup> Návrh rozhodnutí, příloha V.

<sup>11</sup> Viz zejména stanovisko skupiny WP 29 č. 1/2016, oddíl 2.2.6 písm. a).

<sup>12</sup> Návrh rozhodnutí, 195. bod odůvodnění.

štitu EU-USA na ochranu soukromí výrazně vylepšen. Na rozdíl od předchozího právního rámce, který nezakládá práva pro fyzické osoby z EU, jak výslovně uvedl SDEU, nový dekret EO 14086 takové nároky vytváří a poskytuje více záruk pro nezávislost odvolacího soudu pro ochranu údajů a účinnější pravomoci k nápravě porušení.

Při porovnávání dodatečných záruk obsažených v dekretu EO 14086 s evropskými základními zárukami, které EDPB formuloval jako standard vypracovaný na základě judikatury SDEU a Evropského soudu pro lidská práva (ESLP), určil EDPB ve svém posouzení i přesto řadu bodů, které vyžadují další objasnění či pozornost, případně vzbuzují obavy. Tyto body odrážejí skutečnost, že i když EDPB založil své stanovisko na rozhodnutí ve věci Schrems II, rozsah jeho posouzení nutně zahrnuje i úvahy, které přesahují rámec konkrétních zjištění v rozsudku ve věci Schrems II.

EDPB považuje za nutné dále vyjasnit zejména otázky týkající se „dočasného hromadného shromažďování“ a dalšího uchování a šíření údajů shromážděných (v rámci hromadného shromažďování) v právním rámci USA.

Vzhledem k tomu, že test toho, co v zásadě představuje rovnocennost, není testem totožnosti, a k tomu, že byly posíleny záruky obsažené v novém právním rámci týkajícím se signálového zpravodajství, zaměřuje se hlavní pozornost a obavy EDPB na posouzení záruk jako celku na základě holistického přístupu vztahujícího se na záruky pro celý cyklus zpracování od shromažďování údajů po jejich šíření a včetně prvků dohledu a nápravných opatření.

V tomto ohledu zdůrazňuje EDPB tato zjištění:

EDPB sice uznává, že dekret EO 14086 zavádí do právního rámce signálového zpravodajství pojmy nezbytnosti a přiměřenosti, avšak zdůrazňuje potřebu úzce monitorovat účinky těchto změn v praxi včetně přezkumu vnitřních politik a postupů provádějících záruky vyplývající z uvedeného dekretu na úrovni agentur.

EDPB rovněž vítá skutečnost, že dekret EO 14086 obsahuje seznam konkrétních účelů, pro které může a nemůže dojít ke shromažďování, přičemž konstatuje, že cíle mohou být aktualizovány o další – nikoli nutně veřejné – cíle s ohledem na nové požadavky v oblasti národní bezpečnosti.

Jako nedostatek stávajícího rámce EDPB zejména uvedl, že právní rámec USA sice umožňuje hromadné shromažďování údajů podle prezidentského dekretu č. 12333, avšak neobsahuje požadavek na předchozí povolení nezávislého orgánu, jak to vyžaduje nejnovější judikatura ESLP, ani nestanoví systematický nezávislý následný přezkum soudem nebo srovnatelně nezávislým orgánem. Pokud jde o předchozí nezávislé povolení dohledu podle § 702 zákona FISA, vyjadřuje EDPB politování nad tím, že Soud FISA (FISA Court, FISC) při certifikaci programu povolujícího zaměření na osoby, které nejsou občany USA, nepřezkoumává žádost o program z hlediska souladu s dekretem EO 14086, přestože zpravodajské orgány, které daný program provádějí, jsou jím vázány. Podle názoru EDPB by měly být zohledněny dodatečné záruky obsažené v tomto dekretu, a to i ze strany FISC. EDPB připomíná, že pro posouzení toho, jak budou prováděny záruky dekretu EO 14086 a jak budou tyto záruky uplatňovány při shromažďování údajů podle § 702 zákona FISA a podle dekretu EO 12333, by byly obzvláště užitečné zprávy Výboru pro dohled nad ochranou soukromí a občanských svobod (PCLOB).

Pokud jde o nápravný mechanismus, EDPB uznává významná zlepšení týkající se pravomocí odvolacího soudu pro ochranu údajů (DPRC) a jeho větší nezávislosti v porovnání s ombudsmanem. EDPB rovněž uznává dodatečné záruky stanovené v novém nápravném mechanismu, jako je například úloha zvláštních advokátů, která zahrnuje obhajobu zájmů stěžovatele, jakož i přezkum nápravného mechanismu výborem PCLOB. Přestože EDPB zohledňuje povahu národní bezpečnosti a záruky

stanovené v dekretu EO 14086, je znepokojen obecným uplatňováním standardního vyjádření soudu DPRC, v jehož rámci se stěžovateli oznamuje, že buď nebyla zjištěna žádná zahrnutá porušení, nebo že bylo vydáno rozhodnutí vyžadující náležitou nápravu, a proti němuž se ani v jednom případě nelze odvolat. Vzhledem k významu nápravného mechanismu vyzývá EDPB Komisi, aby úzce monitorovala fungování tohoto mechanismu v praxi.

EDPB očekává, že Komise dostojí svému závazku pozastavit, zrušit nebo změnit rozhodnutí o odpovídající ochraně z naléhavých důvodů, zejména pokud by se výkonná moc USA rozhodla omezit záruky obsažené v uvedeném dekretu<sup>13</sup>.

Z celkového hlediska EDPB pozitivně hodnotí podstatná zlepšení, která uvedený dekret přináší v porovnání s předchozím právním rámcem, zejména pokud jde o zavedení zásad nezbytnosti a přiměřenosti a individuálního nápravného mechanismu pro subjekty údajů v EU. Vzhledem k vyjádřeným obavám a požadovaným vysvětlením EDPB navrhuje, aby byly tyto obavy řešeny a aby Komise poskytla požadovaná vysvětlení s cílem lépe odůvodnit návrh rozhodnutí a zajistit pozorné monitorování konkrétního provádění tohoto nového právního rámce a zejména záruk, které poskytuje, v budoucích společných přezkumech.

---

<sup>13</sup> Návrh rozhodnutí, 212. bod odůvodnění.

## Obsah

1	ÚVOD.....	9
1.1	Rámec USA pro ochranu údajů.....	9
1.2	Rozsah posouzení ze strany EDPB.....	11
1.3	Obecné připomínky a obavy .....	13
1.3.1	Posouzení vnitrostátního práva .....	13
1.3.2	Mezinárodní závazky, které USA přijaly.....	13
1.3.3	Pokrok v oblasti právních předpisů USA o ochraně údajů.....	14
1.3.4	Oblast působnosti návrhu rozhodnutí.....	14
1.3.5	Omezení povinnosti dodržovat zásady rámce pro ochranu údajů.....	14
1.3.6	Změny týkající se „štitu na ochranu soukromí“ .....	15
1.3.7	Nejasnosti v dokumentech rámce pro ochranu údajů .....	15
2	OBECNÉ ASPEKTY OCHRANY ÚDAJŮ.....	16
2.1	Základní zásady.....	16
2.1.1	Pojmy .....	16
2.1.2	Zásada omezení účelu.....	17
2.1.3	Právo na přístup, opravu, výmaz a námitku.....	17
2.1.4	Omezení dalšího předávání.....	18
2.1.5	Automatizované rozhodování a profilování .....	19
2.2	Procesní a donucovací mechanismy.....	20
2.3	Mechanismy nápravy .....	21
3	PŘÍSTUP K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM Z EVROPSKÉ UNIE A JEJICH POUŽITÍ ORGÁNY VEŘEJNÉ MOD V USA .....	22
3.1	Přístup k osobním údajům a jejich použití pro účely prosazování trestního práva .....	22
3.1.1	Přístup donucovacích orgánů k osobním údajům by měl být založen na jasných, přesných a přístupných pravidlech .....	22
3.1.2	Nutnost prokázat nezbytnost a přiměřenost s ohledem na sledované legitimní cíle .....	23
3.1.3	Měl by existovat mechanismus nezávislého dohledu .....	25
3.1.4	Fyzické osoby musí mít k dispozici účinné prostředky nápravy .....	25
3.1.5	Další využití shromážděných informací .....	26
3.2	Přístup a použití pro účely národní bezpečnosti.....	27
3.2.1	Záruka A – Zpracování by mělo být v souladu se zákonem a mělo by být založeno na jasných, přesných a přístupných pravidlech.....	28
3.2.2	Záruka B – Nutnost prokázat nezbytnost a přiměřenost s ohledem na sledované legitimní cíle	31
3.2.3	Záruka C – Dohled .....	41

3.2.4	Záruka D – Fyzické osoby musí mít k dispozici účinné opravné prostředky.....	45
4	PROVÁDĚNÍ A MONITOROVÁNÍ NÁVRHU ROZHODNUTÍ.....	53



## Evropský sbor pro ochranu údajů

### Evropský sbor pro ochranu údajů přijal toto prohlášení:

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“)<sup>1</sup>,

s ohledem na Dohodu o EHP, a zejména na přílohu XI a protokol 37 této dohody ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018<sup>2</sup>,

s ohledem na články 12 a 22 svého jednacího řádu,

### PŘIJAL NÁSLEDUJÍCÍ STANOVISKO

## 1 ÚVOD

### 1.1 Rámec USA pro ochranu údajů

1. Spojené státy americké (dále jen „USA“) a Evropská unie (dále jen „EU“) mají odlišné přístupy k soukromí a ochraně údajů. Zatímco v EU představují soukromí a ochrana údajů základní práva zaručená v článcích 7 a 8 Listiny základních práv Evropské unie, v USA se k ochraně údajů obecně přistupuje z hlediska ochrany spotřebitele. V důsledku toho se regulační přístupy v USA a EU liší<sup>3</sup>.
2. Na rozdíl od komplexního přístupu EU, který se odráží v GDPR, neexistuje v USA na federální úrovni žádný komplexní obecný zákon o ochraně údajů. Ochrana soukromí v USA je realizována spíše na základě odvětvového a státního přístupu. Na některá konkrétní odvětví se tak vztahují konkrétní zákony, např.:
  - zákon o přenositelnosti zdravotního pojištění a o související odpovědnosti (Health Insurance Portability and Accountability Act, HIPAA)<sup>4</sup>

---

<sup>1</sup> 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 (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

<sup>2</sup> Pokud se v tomto stanovisku hovoří o „členských státech“, rozumějí se tím „členské státy EHP“.

<sup>3</sup> Viz rovněž návrh prováděcího nařízení Komise podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů podle rámce EU-USA pro ochranu údajů, zveřejněný dne 13. prosince 2022 (dále jen „návrh rozhodnutí“), příloha I oddíl I.

<sup>4</sup> Zákon o přenositelnosti zdravotního pojištění a o související odpovědnosti (Health Insurance Portability and Accountability Act, HIPAA) z roku 1996 je federální zákon USA. Vytváří vnitrostátní normy na ochranu citlivých zdravotních informací o pacientech. Cílem zákona HIPAA je odpovídajícím způsobem chránit zdravotní informace týkající se fyzických osob a zároveň umožnit tok zdravotních informací pro účely poskytování a podpory vysoce kvalitní zdravotní péče. HIPAA upravuje používání a zveřejňování zdravotních údajů subjekty, na které se vztahuje pravidlo o ochraně soukromí. Obsahuje také normy pro práva fyzických osob, které jim umožňují porozumět, jakým způsobem jsou používány jejich zdravotní údaje, a mít nad tímto používáním kontrolu.

<https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>; <https://www.justice.gov/opcl/privacy-act-1974>.

- zákon o ochraně soukromí dětí na internetu (Children's Online Privacy Protection Act, COPPA)<sup>5</sup>
  - zákon Gramma, Leache a Blileyho (Gramm-Leach-Bliley Act, GLBA)<sup>6</sup>
3. V oblasti přístupu vlády k osobním údajům předávaným z EU do USA platí řada různých právních základů, omezení a záruk. Právní postupy pro přístup k informacím pro účely vymáhání práva vyplývají buď přímo z Ústavy Spojených států amerických (čtvrtý dodatek), ze zákonných a procesních předpisů, nebo ze směrnic a politik Ministerstva spravedlnosti USA na federální úrovni nebo na úrovni jednotlivých států. Přístup k informacím pro účely národní bezpečnosti upravuje několik právních nástrojů, zejména zákon o dohledu nad zahraniční informační službou (Foreign Intelligence Surveillance Act, FISA), prezidentský dekret č. 12333, nedávno přijatý prezidentský dekret č. 14086, jakož i nařízení ministra spravedlnosti<sup>7</sup>, kterým se zřizuje odvolací soud pro ochranu údajů (DPRC).
  4. Dne 13. prosince 2022 vydala Komise návrh prováděcího rozhodnutí Komise podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů podle rámce EU-USA pro ochranu údajů (dále jen „návrh rozhodnutí“), jehož příloha obsahuje rámec EU-USA pro ochranu údajů (dále jen „rámec pro ochranu údajů“). Z výše uvedených důvodů není tento návrh rozhodnutí založen na konkrétním a komplexním federálním právním rámci, ale na rámci pro ochranu údajů.
  5. Rámec pro ochranu údajů je vymezen takto: *„Ministerstvo obchodu USA (dále jen „ministerstvo“) v rámci své zákonné pravomoci pěstovat, podporovat a rozvíjet mezinárodní obchod vydává zásady rámce EU-USA pro ochranu údajů včetně doplňkových zásad (dále společně též „zásady“) a přílohy I těchto zásad (dále též „příloha I“) (hlava 15 zákoníku USA (United States Code, U.S.C.) § 1512“*<sup>8</sup>.
  6. Vypracování uvedených zásad (dále jen „zásady rámce pro ochranu údajů“) probíhalo na základě konzultací s Evropskou komisí (dále jen „Komise“), s představiteli průmyslu a s dalšími zúčastněnými stranami za účelem dosažení cíle, jímž je usnadnění obchodu mezi EU a USA<sup>9</sup> a zároveň zajištění toho, aby byla subjektům údajů poskytnuta úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany zaručené v EU.
  7. Zásady rámce pro ochranu údajů jsou popsány jako „klíčová součást“ rámce pro ochranu údajů. Na jedné straně poskytují „mechanismus připravený k okamžitému použití“ pro předávání údajů z EU do

---

<sup>5</sup> Hlavním cílem zákona COPPA je umožnit rodičům kontrolu nad tím, jaké osobní informace jsou od jejich dětí mladších 13 let shromažďovány provozovateli internetových stránek a on-line služeb zaměřených na děti (včetně mobilních aplikací a zařízení pro internet věci, jako jsou například chytré hračky) nebo stránek pro širokou veřejnost. Zákon COPPA vyžaduje, aby tito provozovatelé rodiče uvědomili a získali jejich ověřitelný souhlas. To platí i pro údaje od nezletilých cizinců, pokud jsou dané internetové stránky nebo služby provozovány v USA a vztahuje se na ně zákon COPPA. Současně se tyto předpisy vztahují i na internetové stránky a služby se sídlem v zahraničí, jestliže se zaměřují na děti v USA. Viz: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions> a návrh rozhodnutí, příloha IV, s. 3.

<sup>6</sup> Jedním z cílů zákona Gramma, Leache a Blileyho (GLBA) je chránit soukromí spotřebitelů ve finančním odvětví. Zákon GLBA vyžaduje, aby finanční instituce vysvětlily svým zákazníkům, jaké jsou jejich postupy sdílení informací, a aby vytvořily záruky na ochranu informací o zákaznících (např. pro společnosti regulované komisí FTC podle pravidla FTC o ochranných opatřeních). <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>

<sup>7</sup> Dekret ministra spravedlnosti č. 5517-2022, kterým se mění předpisy Ministerstva spravedlnosti USA podle povolení a pokynů dekretu EO 14086.

<sup>8</sup> Návrh rozhodnutí, příloha I oddíl I.

<sup>9</sup> Tamtéž.

USA. Na druhé straně jsou osobní údaje předávané z EU do USA zabezpečeny a chráněny tak, jak to vyžaduje právo EU.

8. Rámec pro ochranu údajů je použitelný pouze pro ty organizace v USA, které provedou autocertifikaci podle požadavků tohoto rámce (dále jen „organizace podle rámce pro ochranu údajů“). Prozatím je to možné pouze tehdy, pokud spadají do pravomoci Federální obchodní komise (Federal Trade Commission, FTC) nebo ministerstva dopravy. V budoucnu by mohly být do budoucí přílohy doplněny další zákonem zřízené orgány s pravomocí dohlížet na provádění zásad rámce pro ochranu údajů.
9. Zásady rámce pro ochranu údajů vysvětlují, že podmínky tohoto rámce může vymáhat i) FTC podle § 5 zákona o Federální obchodní komisi (FTC Act), který zakazuje nekalé nebo klamavé jednání při obchodování nebo v souvislosti s obchodem<sup>10</sup>, ii) ministerstvo dopravy podle hlavy 49 U.S.C. § 41712, který zakazuje, aby se letecký dopravce nebo prodejce letenek při prodeji letenek či v letecké dopravě dopouštěl nekalých či klamavých praktik, nebo je lze vymáhat iii) podle jiných zákonů nebo předpisů, podle nichž je takové jednání zakázáno.
10. V zásadách rámce pro ochranu údajů se poukazuje na to, že jejich uplatněním není dotčeno ani GDPR, ani stávající povinnosti týkající se ochrany soukromí, které jinak platí podle práva USA.

## 1.2 Rozsah posouzení ze strany EDPB

11. Návrh rozhodnutí odráží hodnocení rámce pro ochranu údajů provedené Komisí, které je výsledkem diskusí s vládou USA. V souladu s čl. 70 odst. 1 písm. s) GDPR se od EDPB očekává vypracování stanoviska ke zjištění Komise, pokud jde o odpovídající úroveň ochrany ve třetí zemi, a v případě potřeby i předložení návrhů k řešení případných problémů.
12. EDPB vítá provedené aktualizace zásad rámce pro ochranu údajů<sup>11</sup>, které budou představovat závazný právní rámec pro organizace podle rámce pro ochranu údajů. EDPB však konstatuje, že zásady rámce pro ochranu údajů zůstávají v podstatě stejné jako zásady podle štítu na ochranu soukromí<sup>12</sup> (z nichž vycházely každoroční společné přezkumy pracovní skupiny zřízené podle článku 29 a EDPB). Zásady rámce pro ochranu údajů jsou rovněž do značné míry totožné se zásadami obsaženými v návrhu štítu na ochranu soukromí, na němž pracovní skupina zřízená podle článku 29 založila své stanovisko z roku 2016<sup>13</sup> (dále jen „stanovisko skupiny WP 29 č. 1/2016“). U zásad rámce pro ochranu údajů, které se podstatně nezměnily, nepovažuje EDPB za nutné opakovat všechny připomínky, které již dříve vnesla pracovní skupina zřízená podle článku 29. EDPB se rozhodl zaměřit se na konkrétní aspekty, které dnes s ohledem na vývoj právního a technologického prostředí považuje za ještě relevantnější.
13. Kromě toho se v souladu s judikaturou SDEU<sup>14</sup> velmi významná část této analýzy týká právního režimu přístupu vlády k osobním údajům předávaným do USA.

---

<sup>10</sup> Hlava 15 U.S.C. § 45 písm. a).

<sup>11</sup> Například objasnění, že údaje kódované pomocí klíče představují osobní údaje.

<sup>12</sup> Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí (Úř. věst. L 207, 1.8.2016, s. 1).

<sup>13</sup> Stanovisko pracovní skupiny pro ochranu údajů zřízené podle článku 29 č. 1/2016 k návrhu rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí, přijaté dne 13. dubna 2016 (dále jen „stanovisko skupiny WP 29 č. 1/2016“).

<sup>14</sup> Jedná se zejména o rozsudek Soudního dvora ze dne 6. října 2015 ve věci Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, a rozsudek Soudního dvora ze dne 16. července 2020

14. EDPB ve svém posouzení zohlednil platný evropský rámec pro ochranu údajů včetně článků 7, 8 a 47 Listiny základních práv EU (dále jen „Listina“), které chrání právo 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), který chrání právo na respektování soukromého a rodinného života. Kromě výše uvedeného vzal EDPB v úvahu požadavky GDPR, příslušnou judikaturu a referenční rámec pro odpovídající ochranu přijatý EDPB (dále jen „referenční rámec GDPR pro odpovídající ochranu“)<sup>15</sup>.
15. Cílem této analýzy je poskytnout Komisi stanovisko k posouzení odpovídající úrovně ochrany poskytované rámcem pro ochranu údajů. Koncept „odpovídající úrovně ochrany“ existoval již ve směrnici 95/46 a SDEU jej dále rozvinul. Je proto důležité připomenout standard stanovený Soudním dvorem v rozsudcích ve věcech Schrems I<sup>16</sup> (zneplatnění zásad „bezpečného přístavu“) a Schrems II<sup>17</sup> (zneplatnění štítu na ochranu soukromí).
16. Ve svém rozsudku ve věci Schrems I Soudní dvůr rozhodl, že ačkoli „úroveň ochrany“ ve třetí zemi musí být „v zásadě rovnocenná“ úrovni ochrany zaručené v EU, „prostředky, které tato třetí země využívá v tomto směru k zajištění takovéto úrovně ochrany, [se] mohou lišit od prostředků zavedených v rámci EU“<sup>18</sup>. Cílem tedy není kopírovat legislativu EU krok za krokem, nýbrž stanovit základní a klíčové požadavky této legislativy. Odpovídající úroveň lze dosáhnout kombinací práv subjektů údajů a povinností subjektů, které zpracovávají osobní údaje 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<sup>19</sup>.
17. SDEU ve svém rozhodnutí ve věci Schrems II konstatoval, že zákony, na jejichž základě mohou zpravodajské orgány USA získat přístup k osobním údajům předaným do USA (§ 702 zákona FISA / EO 12333), nepřiměřeně omezují práva zakotvená v článcích 7 a 8 Listiny základních práv EU (dále jen „Listina“), a nejsou tedy upravena takovým způsobem, aby odpovídala požadavkům, které jsou v zásadě rovnocenné požadavkům vyžadovaným v unijním právu podle čl. 52 odst. 1 druhé věty Listiny<sup>20</sup>.
18. SDEU navíc uvedl, že předchozí právní rámec neposkytoval záruky v zásadě rovnocenné zárukám vyžadovaným v článku 47 Listiny, neboť mechanismus ombudsmana nemůže kompenzovat skutečnost, že ani prezidentská směrnice č. 28 (PPD-28), ani dekret EO 12333 neposkytují osobám,

---

ve věci Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

<sup>15</sup> Pracovní skupina zřízená podle článku 29, Referenční rámec pro odpovídající ochranu, WP 254 rev. 01 ze dne 28. listopadu 2017, v posledním znění přijatém dne 6. února 2018, schválený EDPB dne 25. května 2018 (dále jen „referenční rámec GDPR pro odpovídající ochranu“).

<sup>16</sup> Rozsudek Soudního dvora ze dne 6. října 2015 ve věci Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (dále jen „rozsudek SDEU ve věci Schrems I“).

<sup>17</sup> Rozsudek Soudního dvora ze dne 16. července 2020 ve věci Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (dále jen „rozsudek SDEU ve věci Schrems II“).

<sup>18</sup> Rozsudek SDEU ve věci Schrems I, body 73–74.

<sup>19</sup> Referenční rámec GDPR pro odpovídající ochranu, s. 2.

<sup>20</sup> Rozsudek SDEU ve věci Schrems II, body 184–185.

které nejsou občany USA, účinný prostředek nápravy<sup>21</sup>. Ombudsman nebyl nezávislý na výkonné moci a neměl pravomoc přijímat závazná rozhodnutí ve vztahu ke zpravodajským službám USA<sup>22</sup>.

19. Dekret EO 14086, který obecně nahrazuje směrnici PPD-28, zavedl dva nové požadavky podle práva USA, které jsou odrazem rozsudku SDEU ve věci Schrems II: na jedné straně to, že činnosti signálového zpravodajství se provádějí pouze v rozsahu nezbytném ke shromažďování podle uznaných zpravodajských priorit a pouze v takovém rozsahu a takovým způsobem, který je přiměřený těmto uznaným zpravodajským prioritám, a na straně druhé nápravný mechanismus.
20. V tomto stanovisku EDPB posuzuje zejména to, do jaké míry rámec pro ochranu údajů i nedávno přijatý dekret EO 14086 účinně reagují na zjištění, která SDEU uvedl ve svém rozsudku.

### 1.3 Obecné připomínky a obavy

#### 1.3.1 Posouzení vnitrostátního práva

21. EDPB si je vědom toho, že posouzení obsažené v návrhu rozhodnutí se týká zásad rámce pro ochranu údajů. EDPB by nicméně uvítal určité informace o právním kontextu USA, v němž organizace podle rámce pro ochranu údajů působí. To by umožnilo lépe porozumět interakci rámce pro ochranu údajů s právem USA. Například v příloze I oddíle I<sup>23</sup> je stanoveno, že zásady rámce pro ochranu údajů „[...] *neomezují povinnosti chránit soukromí, které jinak platí podle práva USA*“, aniž by v ní tyto povinnosti byly popsány.

#### 1.3.2 Mezinárodní závazky, které USA přijaly

22. Podle čl. 45 odst. 2 písm. c) GDPR a referenčního rámce GDPR pro odpovídající ochranu musí vzít Komise při posuzování odpovídající úrovně ochrany ve třetí zemi v úvahu, mimo jiné, mezinárodní závazky, které daná třetí země přijala, nebo jiné závazky vyplývající z účasti této třetí země v mnohostranných či regionálních systémech, zejména pokud jde o ochranu osobních údajů, jakož i plnění těchto povinností.
23. USA jsou smluvní stranou několika mezinárodních dohod, které zaručují právo na soukromí, jako je Mezinárodní pakt o občanských a politických právech (článek 17), Úmluva o právech osob se zdravotním postižením (článek 22) a Úmluva o právech dítěte (článek 16). Kromě toho USA jako člen OECD dodržují rámec OECD pro ochranu údajů, zejména obecné zásady, kterými se řídí ochrana soukromí a přeshraniční toky osobních údajů. Dne 14. prosince 2022 přijali ministři a vysocí představitelé členských zemí OECD a Evropské unie „Prohlášení OECD o přístupu vlády k osobním údajům v držení subjektů soukromého sektoru“. USA jsou také smluvní stranou Budapešťské úmluvy o kyberkriminalitě.
24. Kromě toho jsou USA členem systému pravidel přeshraniční ochrany soukromí (CBPR) zemí Asijsko-tichomořské hospodářské spolupráce (APEC), což je vládou podporovaná certifikace ochrany osobních údajů, k níž se společnosti mohou připojit, aby prokázaly soulad s mezinárodně uznávanými pravidly ochrany soukromí. Tato pravidla ochrany soukromí schválili vedoucí představitelé APEC.
25. EDPB rovněž bere na vědomí účast USA jako pozorovatelského státu na činnosti poradního výboru Úmluvy Rady Evropy č. 108.

---

<sup>21</sup> Rozsudek SDEU ve věci Schrems II, bod 192.

<sup>22</sup> Rozsudek SDEU ve věci Schrems II, bod 195.

<sup>23</sup> Návrh rozhodnutí, příloha I oddíl I poslední věta.

26. EDPB dále bere na vědomí a vítá trvalé zapojení orgánů USA do formátu nově zavedeného v roce 2021, „kulatého stolu orgánů skupiny G7 pro ochranu údajů a soukromí“ (Roundtable of G7 Data Protection and Privacy Authorities), kde se setkávají nezávislé orgány pro ochranu údajů a soukromí zemí G7. Ty v této souvislosti podpořily například nejnovější komuniké kulatého stolu orgánů skupiny G7 pro ochranu údajů a soukromí<sup>24</sup>, přijaté dne 8. září 2022 v německém Bonnu, které se zaměřilo na koncept „volného toku dat na základě důvěry“ (Data Free Flow with Trust).

### 1.3.3 Pokrok v oblasti právních předpisů USA o ochraně údajů

27. EDPB bere na vědomí zejména vývoj právních předpisů v oblasti ochrany osobních údajů v USA na úrovni jednotlivých států. EDPB vítá přijetí právních předpisů na ochranu údajů, které vstoupily nebo do roku 2023 vstoupí v platnost v pěti státech (Kalifornie, Colorado, Connecticut, Virginie a Utah)<sup>25</sup>.
28. EDPB rovněž konstatuje, že příslušné iniciativy pro přijetí dalších státních zákonů již byly zahájeny i mnoha dalších státech USA.
29. EDPB dále výslovně vítá úsilí ohledně dvoustranné iniciativy týkající se federálního zákona o ochraně údajů, amerického zákona o ochraně údajů a soukromí (American Data Privacy and Protection Act, DPPA).

### 1.3.4 Oblast působnosti návrhu rozhodnutí

30. Podle článku 1 návrhu rozhodnutí dospěla Komise k závěru, že USA zajišťují odpovídající úroveň ochrany osobních údajů předávaných z EU organizacím v USA, které jsou uvedeny na „seznamu podle rámce pro ochranu údajů“, který spravuje a zveřejňuje Ministerstvo obchodu USA v souladu s oddílem I bodem 3 přílohy I<sup>26</sup>.
31. Rámec pro ochranu údajů je k dispozici společnostem, které spadají do pravomoci Federální obchodní komise (FTC) nebo ministerstva dopravy. Upozorňuje se, že v budoucnu mohou být připojeny další zákonem zřízené subjekty USA s obdobnými pravomocemi<sup>27</sup>.

### 1.3.5 Omezení povinnosti dodržovat zásady rámce pro ochranu údajů

32. Příloha I oddíl I bod 5 stanoví, že dodržování zásad rámce pro ochranu údajů organizacemi podle tohoto rámce může být omezeno mimo jiné i) v rozsahu nezbytném pro splnění soudního příkazu nebo pro

---

<sup>24</sup> Roundtable of G7 Data Protection and Privacy Authorities, Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces (Kulatý stůl orgánů skupiny G7 pro ochranu údajů a soukromí, Podpora volného toku dat na základě důvěry a sdílení znalostí o vyhlídkách mezinárodních datových prostor), 8. září 2022,

[https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?\\_\\_blob=publicationFile&v=1](https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1).

<sup>25</sup> California Consumer Privacy Act (zákon státu Kalifornie o ochraně soukromí spotřebitelů) (2018; účinný od 1. ledna 2020); California Privacy Rights Act (zákon státu Kalifornie o právech na ochranu soukromí) (2020; plně funkční od 1. ledna 2023); Colorado Privacy Act (zákon státu Colorado o ochraně soukromí) (2021; účinný od 1. července 2023); Connecticut Data Privacy Act (zákon státu Connecticut o ochraně údajů) (2022; účinný od 1. července 2023); Virginia Consumer Data Protection Act (zákon státu Virginie o ochraně údajů spotřebitelů) (2021; účinný od 1. ledna 2023); Utah Consumer Privacy Act (zákon státu Utah o ochraně soukromí spotřebitelů) (2022; účinný od 31. prosince 2023).

<sup>26</sup> Návrh rozhodnutí, závěrečné úvahy, článek 1, s. 57. EDPB má za to, že návrh rozhodnutí se nebude vztahovat na předávání údajů od subjektů, které se nacházejí mimo EU, ale podléhají GDPR na základě čl. 3 odst. 2 GDPR, certifikovaným subjektům v USA.

<sup>27</sup> Návrh rozhodnutí, příloha I oddíl I bod 2.

splnění požadavků veřejného zájmu, prosazování práva<sup>28</sup> nebo národní bezpečnosti<sup>29</sup> (včetně případů, kdy zákon nebo správní nařízení vytvářejí protichůdné závazky) a ii) zákonem, soudním příkazem nebo správním nařízením, které zakládají výslovná zmocnění, za předpokladu, že při výkonu takového zmocnění může organizace podle rámce pro ochranu údajů prokázat, že nedodržení zásad rámce pro ochranu údajů z její strany je omezeno na rozsah nezbytný pro splnění nadřazených oprávněných zájmů, jimž má takové zmocnění sloužit.

33. Bez plné znalosti práva USA na federální i státní úrovni je pro EDPB obtížné podrobně posoudit rozsah výjimek uvedených v tomto odstavci. EDPB proto doporučuje, aby Komise do návrhu rozhodnutí zahrnula objasnění rozsahu výjimek včetně platných záruk podle práva USA, s cílem lépe určit dopad těchto výjimek na úroveň ochrany subjektů údajů. EDPB rovněž zdůrazňuje, že Komise by měla být informována o uplatňování a přijetí jakéhokoli zákona nebo správního nařízení, které by ovlivnily dodržování zásad rámce pro ochranu údajů, a měla by toto uplatňování a přijímání monitorovat.

#### 1.3.6 Změny týkající se „štitu na ochranu soukromí“

34. EDPB vítá úsilí vynaložené na řešení požadavků vyplývajících z rozsudku ve věci Schrems II. EDPB by nicméně uvítal, kdyby se při příležitosti jednání o rámci pro ochranu údajů řešilo také více problémů zjištěných i) ve stanovisku skupiny WP 29 č. 1/2016 a ii) v minulých společných přezkumech<sup>30</sup>.
35. EDPB rovněž konstatuje, že navzdory řadě změn a dodatečných vysvětlení uvedených v bodech odůvodnění návrhu rozhodnutí zůstávají zásady rámce pro ochranu údajů, které musí organizace podle rámce pro ochranu údajů dodržovat, v podstatě beze změny, pokud jde o zásady použitelné v rámci štitu na ochranu soukromí.

#### 1.3.7 Nejasnosti v dokumentech rámce pro ochranu údajů

36. EDPB konstatuje, že vzhledem ke struktuře příloh a jejich číslování je poměrně obtížné tyto informace nalézt a odkazovat na ně. To přispívá k celkově složité prezentaci nového rámce, který ve svých přílohách shrnuje dokumenty různé právní hodnoty a ne vždy napomáhá dobrému chápání zásad rámce pro ochranu údajů ze strany subjektů údajů, organizací podle rámce pro ochranu údajů a orgánů EU pro ochranu údajů.
37. EDPB rovněž zdůrazňuje, že terminologie by měla být používána v celém rámci pro ochranu údajů jednotně. V současné době tomu tak není například v případě pojmu „zpracování“. Některé části rámce pro ochranu údajů totiž uvádějí výčet některých druhů operací zpracování údajů namísto použití výrazu „zpracování“ To může vést k právní nejistotě a možným mezerám v ochraně<sup>31</sup>.

---

<sup>28</sup> Další připomínky k používání osobních údajů, na které se vztahuje rámec EU-USA pro ochranu údajů, pro účely prosazování práva jsou uvedeny v oddíle 3.1 tohoto stanoviska.

<sup>29</sup> Další připomínky k používání osobních údajů, na které se vztahuje rámec EU-USA pro ochranu údajů, pro účely národní bezpečnosti jsou uvedeny v oddíle 3.2 tohoto stanoviska.

<sup>30</sup> Každoroční přezkumy: štit EU-USA na ochranu soukromí – první každoroční společný přezkum, WP 255, zpráva pracovní skupiny zřízené podle článku 29 přijatá dne 28. listopadu 2017 (dále jen „první zpráva o společném přezkumu“); štit EU-USA na ochranu soukromí – druhý každoroční společný přezkum, zpráva EDPB přijatá dne 22. ledna 2019 (dále jen „druhá zpráva o společném přezkumu“); štit EU-USA na ochranu soukromí – třetí každoroční společný přezkum, zpráva EDPB přijatá dne 12. listopadu 2019 (dále jen „třetí zpráva o společném přezkumu“).

<sup>31</sup> Například i) podle znění přílohy I oddílu III bodu 6 písm. f) návrhu rozhodnutí by zásady rámce pro ochranu údajů byly použitelné pouze tehdy, pokud organizace „uchovává, používá nebo předává“ obdržené údaje (tj. nikoli pro jiné operace, na které se vztahuje pojem „zpracování“, jako je například shromažďování,

38. EDPB vítá, že v rámci pro ochranu údajů jsou uvedeny definice některých používaných pojmů<sup>32</sup>. To však neplatí pro některé jiné základní pojmy, přinejmenším pro pojem „zmocněnec“ nebo „zpracovatel“, které podle názoru EDPB vyžadují jasnou a konkrétní definici v příloze I oddíle I bodě 8 rámce pro ochranu údajů a USA i EU by se na nich měly shodnout, aby se v pozdější fázi předešlo nejasnostem pro organizace podle rámce pro ochranu údajů, které se spoléhají na rámec pro ochranu údajů, dozorové úřady a širokou veřejnost.
39. Pokud jde o otázku rozdílných výkladů pojmu „údaje o lidských zdrojích“ v EU a USA, EDPB souhlasí s třetí zprávou Komise o přezkumu ohledně cíle pokračovat v diskusích s orgány USA<sup>33</sup>.

## 2 OBECNÉ ASPEKTY OCHRANY ÚDAJŮ

### 2.1 Základní zásady

#### 2.1.1 Pojmy

40. Na základě referenčního rámce GDPR pro odpovídající ochranu by v právním rámci třetí země měly existovat základní koncepty a/nebo zásady ochrany údajů. Přestože není nutné, aby kopírovaly terminologii GDPR, měly by odrážet pojmy zakotvené v evropských právních předpisech o ochraně údajů a být s nimi v souladu. GDPR například obsahuje mimo jiné následující důležité pojmy: „osobní údaje“, „zpracování osobních údajů“, „správce údajů“, „zpracovatel údajů“, „příjemce“ a „citlivé údaje“. EDPB vítá, že definice pojmů „osobní údaje“, „zpracování“ a „správce“ jsou zahrnuty do rámce pro ochranu údajů, stejně jako tomu bylo v případě štítu na ochranu soukromí.
41. EDPB konstatuje, že rozsah, v jakém se zásady rámce pro ochranu údajů vztahují na organizace podle rámce pro ochranu údajů, které přijímají osobní údaje z EU pro účely „pouhého zpracování“ (označované jako „zmocněnci“ nebo „zpracovatelé“), zůstává nejasný. Rámec pro ochranu údajů nerozlišuje mezi zásadami rámce pro ochranu údajů platnými pro zmocněnce a zásadami rámce pro ochranu údajů platnými pro správce, přičemž některé z povinností obsažených v zásadách rámce pro ochranu údajů nejsou vhodné pro zmocněnce/zpracovatele. Zmocněnec/zpracovatel by například neměl mít možnost poskytovat fyzickým osobám všechny prvky úplného oznámení, jak to vyžaduje zásada oznamovací povinnosti (např. účely, pro které o nich shromažďuje a používá osobní údaje)<sup>34</sup>, protože zmocněnec/zpracovatel nemůže sám určovat prostředky a účely zpracování<sup>35</sup>.

---

za značování, pozměňování, vyhledávání, nahlížení, výmaz), a ii) podle přílohy I oddílu II bodu 4 písm. a) návrhu rozhodnutí by bezpečnost údajů byla vyžadována pouze pro „vytváření, uchovávání, používání nebo šíření“ osobních informací.

<sup>32</sup> Návrh rozhodnutí, příloha I oddíl I bod 8.

<sup>33</sup> Třetí zpráva o společném přezkumu, s. 5, 15–16 a 30; viz také pracovní dokument útvarů Komise připojený ke zprávě Komise Evropskému parlamentu a Radě o třetím každoročním přezkumu fungování štítu EU-USA na ochranu soukromí, s. 17–18.

<sup>34</sup> Návrh rozhodnutí, příloha I oddíl II bod 1 písm. a).

<sup>35</sup> Viz rovněž stanovisko skupiny WP 29 č. 1/2016, s. 16.



### 2.1.2 Zásada omezení účelu

42. Referenční rámec GDPR pro odpovídající ochranu stanoví, v souladu s nařízením GDPR, že osobní údaje by měly být zpracovány pro konkrétní účel a následně by se měly používat k některému z těchto účelů pouze tehdy, pokud to není neslučitelné s účelem zpracování.
43. Zásada integrity údajů a účelového omezení stanoví, že organizace nesmí zpracovávat osobní informace způsobem, který není v souladu s účely, pro které byly shromážděny nebo následně schváleny danou fyzickou osobou<sup>36</sup>. EDPB konstatuje, že v rámci zásady oznamovací povinnosti, zásady možnosti volby a zásady integrity údajů a účelového omezení je používána odlišná terminologie. Jak uvádí pracovní skupina zřízená podle článku 29 a navzdory užitečnému objasnění v bodech odůvodnění návrhu rozhodnutí se v rámci pro ochranu údajů používají pojmy jako „různé účely“, „významně odlišné“ účely nebo „použití, které není v souladu“, aniž by v něm byla obsažena jasná definice těchto pojmů, což by mohlo vést k právní nejistotě.

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

44. V rámci pro ochranu údajů jsou práva subjektů údajů na přístup, opravu a výmaz upravena zásadou práva na přístup<sup>37</sup>.
45. Zásada práva na přístup zůstává v porovnání se štítem EU-USA na ochranu soukromí beze změny. V důsledku toho jsou některé problematické body vyjádřené ve stanovisku skupiny WP 29 č. 1/2016 stále platné, jak je podrobně uvedeno níže.
46. Pokud jde o právo fyzických osob na přístup, považuje EDPB za nezbytné zopakovat, že podrobnosti o povinnosti odpovídat na žádosti fyzických osob by bylo lepší vložit do hlavního textu této zásady (jsou stále popsány pouze v poznámce pod čarou<sup>38</sup>). Také by mělo být jasné, že přístup by měl být poskytován v tom rozsahu, v jakém organizace rámce pro ochranu údajů zpracovává osobní údaje, nejen v jakém je „uchovává“<sup>39</sup>. Podle názoru EDPB by stávající znění mohlo vést k restriktivnímu výkladu práva na přístup.
47. Pokud jde o seznam výjimek z práva na přístup<sup>40</sup>, některé mají stále tendenci vychylovat rovnováhu ve prospěch zájmů organizací podle rámce pro ochranu údajů. EDPB je i nadále znepokojen tím, že v těchto případech zřejmě neexistuje požadavek na zohlednění práv a zájmů fyzických osob<sup>41</sup>.
48. Další výjimkou, ohledně které pracovní skupina zřízená podle článku 29 již dříve vyjádřila znepokojení<sup>42</sup> a která se výboru EDPB jeví jako příliš široká, je výjimka z práva na přístup k veřejně dostupným informacím a informacím z veřejných záznamů<sup>43</sup>. EDPB opakovaně uvedl, že podle práva EU mají subjekty údajů vždy právo na přístup ke svým údajům bez ohledu na to, zda byly tyto osobní údaje zveřejněny či nikoli. Pokud by žádosti o přístup byly zamítnuty z toho důvodu, že údaje byly získány z veřejně dostupných zdrojů nebo veřejných záznamů, ztratily by fyzické osoby možnost kontrolovat správnost těchto údajů a zejména to, zda byly tyto údaje zveřejněny v souladu se zákonem.

---

<sup>36</sup> Návrh rozhodnutí, příloha I oddíl II bod 5.

<sup>37</sup> Návrh rozhodnutí, příloha I oddíl II bod 6 a oddíl III bod 8 písm. a) podbod i).

<sup>38</sup> Návrh rozhodnutí, příloha I oddíl III bod 8 písm. a) podbod i) bod 1 – poznámka pod čarou 14.

<sup>39</sup> Návrh rozhodnutí, příloha I oddíl III bod 8 písm. d) podbod ii).

<sup>40</sup> Návrh rozhodnutí, příloha I oddíl III bod 8 písm. e).

<sup>41</sup> Stanovisko skupiny WP 29 č. 1/2016, bod 2.2.5.

<sup>42</sup> Stanovisko skupiny WP 29 č. 1/2016, bod 2.2.9.

<sup>43</sup> Návrh rozhodnutí, příloha I oddíl III bod 15 písm. d) a e).

49. EDPB připomíná, že právo na přístup je zakotveno v čl. 8 odst. 2 Listiny. I když se nejedná o právo absolutní, má zásadní význam pro právo na ochranu osobních údajů, neboť usnadňuje výkon ostatních práv subjektu údajů, jako je právo na opravu a výmaz a právo vznést námitku<sup>44</sup>.
50. Kromě práva na přístup a výmaz by subjekty údajů měly mít kdykoli ze závažných oprávněných důvodů vztahujících se ke jejich konkrétní situaci právo vznést námitku proti zpracování svých údajů za zvláštních podmínek stanovených v právním rámci třetí země<sup>45</sup>.
51. Zásadou možnosti volby stanoví rámec pro ochranu údajů právo vznést námitku (opt-out) proti zpřístupnění osobních informací třetí straně nebo proti použití osobních informací pro významně odlišný účel<sup>46</sup>. Fyzické osoby mají navíc právo kdykoli vyslovit nesouhlas s používáním svých osobních údajů pro účely přímého marketingu<sup>47</sup>. S výjimkou účelů přímého marketingu však nejsou podrobně popsány způsoby uplatnění práva vznést námitku, zejména lhůty pro uplatnění tohoto práva. EDPB proto vyzývá Komisi, aby objasnila, jak mohou fyzické osoby uplatňovat své právo vznést námitku.
52. Jak je uvedeno ve stanovisku skupiny WP 29 č. 1/2016, Evropský sbor pro ochranu údajů se domnívá, že pouhý odkaz na existenci tohoto práva v zásadách ochrany soukromí nemůže být dostatečný. Měla by být poskytnuta individualizovaná příležitost k uplatnění tohoto práva nejen v případě sdělování nebo opakovaného použití osobních informací. EDPB zdůrazňuje, že v rámci pro ochranu údajů by mělo být poskytováno obecné právo vznést námitku ze závažných legitimních důvodů týkajících se konkrétní situace subjektu údajů. EDPB doporučuje, aby takové právo vznést námitku bylo kdykoli zaručeno a aby toto právo nebylo omezeno na použití údajů pro přímý marketing<sup>48</sup>.
53. Pokud jde o údaje o lidských zdrojích, EDPB oceňuje vysvětlení Komise, pokud jde o uplatňování zásady oznamovací povinnosti a možnosti volby v situaci, kdy certifikovaná organizace v USA hodlá použít údaje o lidských zdrojích pro jiný účel nesouvisející se zaměstnáním, například pro marketingová sdělení<sup>49</sup>. EDPB však trvá na tom, že další zpracovávání údajů o lidských zdrojích pro účely nesouvisející se zaměstnáním bude ve většině případů považováno za neslučitelné s původním účelem a že pokud bude souhlas udělován v souvislosti se zaměstnáním, bude jen zřídka zcela svobodný.
54. EDPB rovněž opakovaně cituje obavy pracovní skupiny zřízené podle článku 29 v souvislosti s výjimkou ze zásad oznamovací povinnosti a možnosti volby pro údaje o lidských zdrojích „*v rozsahu a po dobu nezbytnou k zachování schopnosti organizace povyšovat, jmenovat nebo přijímat jiná podobná personální rozhodnutí*“<sup>50</sup>, což se EDPB jeví jako obecné a vágní<sup>51</sup>.

#### 2.1.4 Omezení dalšího předávání

55. Další předávání osobních údajů původním příjemcem původního předání údajů by mělo být povoleno pouze v případě, že další příjemce (tj. příjemce dalšího předávání) rovněž podléhá pravidlům (včetně smluvních pravidel) zajišťujícím odpovídající úroveň ochrany a řídí se příslušnými pokyny při zpracování údajů jménem správce údajů. Úroveň ochrany fyzických osob, jejichž údaje jsou předávány, nesmí být dalším předáváním narušena. Původní příjemce údajů předávaných z EU odpovídá za zajištění

<sup>44</sup> Stanovisko skupiny WP 29 č. 1/2016, bod 2.2.5.

<sup>45</sup> Referenční rámec GDPR pro odpovídající ochranu, oddíl 3.A.8.

<sup>46</sup> Návrh rozhodnutí, příloha I oddíl II bod 2 písm. a).

<sup>47</sup> Návrh rozhodnutí, příloha I oddíl III bod 12 písm. a).

<sup>48</sup> Stanovisko skupiny WP 29 č. 1/2016, bod 2.2.2.

<sup>49</sup> Návrh rozhodnutí, příloha I oddíl III bod 9 písm. b) podbod i), 15. bod odůvodnění a poznámka pod čarou 27.

<sup>50</sup> Návrh rozhodnutí, příloha I oddíl III bod 9 písm. b) podbod iv).

<sup>51</sup> Stanovisko skupiny WP 29 č. 1/2016, bod 2.2.7.

vhodných záruk pro další předávání údajů, pokud neexistuje rozhodnutí o odpovídající ochraně. Takové další předávání údajů by se mělo uskutečnit pouze pro omezené a konkrétní účely a jen tehdy, pokud existuje pro tento druh zpracování právní důvod<sup>52</sup>.

56. Podle zásady odpovědnosti za další předávání uvedené v rámci pro ochranu údajů může k jakémukoli dalšímu předání dojít pouze k omezeným a konkrétním účelům na základě smlouvy mezi organizací podle rámce pro ochranu údajů a třetí stranou (nebo srovnatelného ujednání v rámci skupiny společností) a jen tehdy, pokud taková smlouva požaduje, aby daná třetí strana poskytovala stejnou úroveň ochrany, jakou poskytují zásady rámce pro ochranu údajů<sup>53</sup>.
57. EDPB by rád znovu zmínil obavy vyjádřené ve stanovisku skupiny WP 29 č. 1/2016 ohledně výjimky z potřeby smlouvy pro vnitroskupinové předávání údajů mezi správci<sup>54</sup>. Pokud jde o údaje o lidských zdrojích, EDPB stále nerozumí zdůvodnění výjimky z povinnosti uzavřít smlouvu s třetí stranou, která je správcem, v případě dalšího předávání za účelem „příležitostných provozních potřeb v rámci zaměstnaneckého vztahu“<sup>55</sup>.
58. EDPB by dále rád zopakoval požadavek pracovní skupiny zřízené podle článku 29<sup>56</sup>, aby organizace vázané tímto rámcem před dalším předáním posoudily, zda závazné požadavky vnitrostátních právních předpisů třetí země, které se vztahují na příjemce, nenaruší kontinuitu ochrany subjektů údajů, jejichž údaje jsou předávány<sup>57</sup>.
59. EDPB tvrdí, že další předávání osobních údajů do třetích zemí by mohlo vést k zásahům do základních práv fyzických osob, a vyzývá Komisi, aby objasnila, že záruky uložené původním příjemcem dovozci ve třetí zemi musí být před dalším předáváním v souvislosti s rámcem pro ochranu údajů účinné s ohledem na právní předpisy třetích zemí<sup>58</sup>.

### 2.1.5 Automatizované rozhodování a profilování

60. K rozhodnutím založeným výhradně na automatizovaném zpracování (automatizované individuální rozhodování), včetně profilování, která mají pro subjekt údajů právní účinky nebo se jej významně dotýkají, může docházet jen za určitých podmínek stanovených v právním rámci třetí země. V evropském rámci k takovým podmínkám patří například potřeba získat výslovný souhlas subjektu údajů nebo nezbytnost takového rozhodnutí pro uzavření smlouvy. Pokud rozhodnutí nespĺňuje takové podmínky stanovené v právním rámci třetí země, měl by mít subjekt údajů právo nestát se subjektem tohoto rozhodnutí. Právo třetí země by mělo v každém případě stanovit nezbytné záruky, včetně práva být informován o konkrétních důvodech, na nichž je rozhodnutí založeno, a o související logice, práva

<sup>52</sup> Referenční rámec GDPR pro odpovídající ochranu, oddíl 3.A.9.

<sup>53</sup> Návrh rozhodnutí, příloha I oddíl II bod 3.

<sup>54</sup> Návrh rozhodnutí, příloha I oddíl III bod 10 písm. b) podbod i), který odkazuje na „jiné vnitroskupinové nástroje (např. programy dodržování předpisů a kontrolní programy)“, které zjevně nemusí být závazné.

<sup>55</sup> Návrh rozhodnutí, příloha I oddíl III bod 9 písm. e) podbod i), který odkazuje na příklady, jako je pojištění.

<sup>56</sup> Stanovisko skupiny WP 29 č. 1/2016, bod 2.2.3, s. 21.

<sup>57</sup> S ohledem na rozsudek ve věci Schrems II EDPB v řadě pokynů a doporučení dále objasnil povinnosti vývozců a dovozců údajů v souvislosti s dalším předáváním; viz doporučení EDPB 1/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU (verze 2.0, přijato dne 18. června 2021); doporučení 2/2020 týkající se evropských základních záruk pro sledovací opatření (přijato dne 10. listopadu 2020); pokyny 4/2021 týkající se kodexů chování jakožto nástrojů pro předávání údajů (verze 2.0, přijato dne 22. února 2022); doporučení 1/2022 týkající se žádosti o schválení a prvků a zásad, které mají být obsaženy v závazných podnikových pravidlech správce (přijato dne 14. listopadu 2022); pokyny 7/2022 o certifikaci jako nástroji pro předávání (přijato po veřejné konzultaci dne 14. února 2023).

<sup>58</sup> Stanovisko skupiny WP 29 č. 1/2016, bod 2.2.3, s. 21.

opravit nepřesné nebo neúplné informace a práva napadnout rozhodnutí, pokud vycházelo z nesprávného skutkového stavu<sup>59</sup>.

61. Rámec pro ochranu údajů neposkytuje žádné zvláštní právní záruky v případech, kdy jsou fyzické osoby subjektem rozhodnutí, která vůči nim zakládají právní účinky nebo která se jich významně dotýkají a která jsou přijata výlučně na základě automatizovaného zpracování údajů určeného k hodnocení určitých rysů jejich osobnosti, například pracovního výkonu, důvěryhodnosti, spolehlivosti nebo chování.
62. Jak již uvádí stanovisko pracovní skupiny zřízené podle článku 29 č. 1/2016 a EDPB ve svých předchozích stanoviscích k rozhodnutím o odpovídající ochraně ve vztahu k Japonsku a Jižní Koreji<sup>60</sup>, EDPB konstatuje, že v tomto ohledu vyžaduje zvláštní pozornost rychlý vývoj v oblasti automatizovaného rozhodování a profilování, který probíhá stále více prostřednictvím technologií umělé inteligence<sup>61</sup>.
63. EDPB bere na vědomí argumenty Komise, podle nichž neexistence zvláštních pravidel pro automatizované rozhodování v rámci pro ochranu údajů pravděpodobně neovlivní úroveň ochrany, pokud jde o osobní údaje, které byly shromážděny v Unii (jelikož jakékoli rozhodnutí založené na automatizovaném zpracování by obvykle přijal správce v Unii, který má přímý vztah s dotčeným subjektem údajů)<sup>62</sup>. Podle názoru EDPB však nelze vyloučit, že by automatizovaného rozhodování o údajích předávaných podle návrhu rozhodnutí mohl využít i správce se sídlem v USA (např. v souvislosti se zaměstnáním, posouzením pracovního výkonu, pojištěním či bydlením).
64. EDPB vítá odkazy Komise na konkrétní záruky, které poskytují příslušné právní předpisy USA v různých oblastech<sup>63</sup>. Podle EDPB se však zdá, že úroveň ochrany fyzických osob se liší podle toho, která odvětvová pravidla – pokud vůbec nějaká – se na danou situaci vztahují. Existuje riziko, že některé situace nebudou pokryty, protože nespádají do oblasti působnosti uvedených zákonů. Kromě toho je obsah práv fyzických osob ve vztahu k automatizovanému rozhodování v jednotlivých aktech popisován různě.
65. EDPB se v této souvislosti domnívá, že jsou v rámci pro ochranu údajů v zájmu poskytnutí dostatečných záruk zapotřebí konkrétní pravidla týkající se automatizovaného rozhodování včetně práva fyzické osoby znát příslušnou logiku, práva napadnout dané rozhodnutí a práva na lidský zásah, pokud se jí rozhodnutí významně dotýká<sup>64</sup>.

## 2.2 Procesní a donucovací mechanismy

66. EDPB konstatuje, že rámec pro ochranu údajů se i nadále spoléhá na systém autocertifikace, i když jej Komise označuje jako systém „certifikace“.

---

<sup>59</sup> Referenční rámec GDPR pro odpovídající ochranu, oddíl 3.B.3.

<sup>60</sup> Stanovisko EDPB 28/2018 k návrhu prováděcího rozhodnutí Evropské komise o odpovídající ochraně osobních údajů v Japonsku, přijaté dne 5. prosince 2018; stanovisko EDPB 32/2021 k návrhu prováděcího rozhodnutí Evropské komise o odpovídající ochraně osobních údajů v Korejské republice, přijaté dne 24. září 2021.

<sup>61</sup> Viz mimo jiné věc C-634/21, OQ v. Land Hessen (SCHUFA Holding a další), žádost o rozhodnutí o předběžné otázce (dosud neuzavřeno).

<sup>62</sup> Návrh rozhodnutí, 33. a 34. bod odůvodnění.

<sup>63</sup> Návrh rozhodnutí, 35. bod odůvodnění.

<sup>64</sup> Viz rovněž třetí zpráva o společném přezkumu, bod 76.

67. EDPB připomíná zlepšení, jichž bylo dosaženo v průběhu společných přezkumů v minulosti. Například pokud jde o úlohu ministerstva obchodu v procesu (opětovné) autocertifikace, sledování toho, jak společnosti dodržují zásady rámce pro ochranu údajů (např. prostřednictvím namátkových kontrol a používání dotazníků týkajících se dodržování zásad), a zjišťování a řešení nepravdivých tvrzení o účasti (např. prostřednictvím vyhledávání na internetu).
68. Pracovní skupina zřízená podle článku 29 a EDPB zároveň vyjádřily obavy ohledně určitých nedostatků v oblasti dohledu nad dodržováním požadavků štítu na ochranu soukromí<sup>65</sup>. EDPB souhlasí zejména se zjištěními Komise po třetím každoročním přezkumu štítu na ochranu soukromí, že kontroly na místě prováděné ministerstvem obchodu v rámci štítu na ochranu soukromí bývaly omezeny na formální požadavky (například že určená kontaktní místa nereagovala nebo že pravidla na ochranu soukromí nebyla v případě určité společnosti dostupná online)<sup>66</sup>. EDPB má za to, že klíčový význam mají kontroly dodržování zásadnějších požadavků.
69. EDPB rovněž připomíná význam účinného dohledu (včetně dodržování základních požadavků) a prosazování rámce pro ochranu údajů. EDPB bude tento aspekt úzce monitorovat, a to i v souvislosti s pravidelnými přezkumy.
70. Pokud jde o prosazování, EDPB bere na vědomí obnovené závazky uvedené v dopisech komise FTC<sup>67</sup> a ministerstva dopravy<sup>68</sup>, v nichž se zavazují upřednostňovat vyšetřování údajných porušení rámce pro ochranu údajů, přijímat vhodná opatření za účelem prosazování práva vůči subjektům, které předkládají nepravdivá nebo klamavá tvrzení o účasti, sledovat výkon rozhodnutí týkajících se porušení rámce pro ochranu údajů a spolupracovat s orgány EU pro ochranu údajů. V tomto ohledu EDPB rovněž uznává, že FTC dle vlastního tvrzení předpokládá, že dále zaměří své úsilí v oblasti prosazování na závažná porušení rámce pro ochranu údajů a že má v úmyslu vyšetřovat (také) z vlastního podnětu. EDPB bude tyto aspekty úzce monitorovat, a to i v souvislosti s pravidelnými přezkumy.

### 2.3 Mechanismy nápravy

71. EDPB vítá skutečnost, že v návrhu rozhodnutí je jasně představeno sedm možností nápravy poskytnutých subjektům údajů z EU, pokud jsou jejich osobní údaje zpracovávány v rozporu s rámcem pro ochranu údajů<sup>69</sup>.
72. Tyto různé odvolací mechanismy jsou zavedeny v souladu s požadavky zásady odvolání, vymáhání a odpovědnosti a doplňkové zásady č. 11 týkající se řešení sporů a vymáhání vydané ministerstvem obchodu a uvedené v příloze I návrhu rozhodnutí<sup>70</sup>.
73. Jak zdůraznila Komise ve svém návrhu rozhodnutí, „*subjektu údajů by měla být poskytnuta účinná správní a soudní ochrana*“<sup>71</sup>. To odráží požadavek uvedený v čl. 45 odst. 2 písm. a) GDPR, podle něhož musí Komise při posuzování odpovídající úrovně ochrany ve třetí zemi vzít v úvahu mimo jiné existenci

---

<sup>65</sup> Třetí zpráva o společném přezkumu, bod 7.

<sup>66</sup> Zpráva Komise Evropskému parlamentu a Radě o třetím každoročním přezkumu fungování štítu EU–USA na ochranu soukromí (COM(2019)495 final ze dne 23. října 2019), s. 4.

<sup>67</sup> Návrh rozhodnutí, příloha IV.

<sup>68</sup> Návrh rozhodnutí, příloha V.

<sup>69</sup> Návrh rozhodnutí, 67. bod odůvodnění.

<sup>70</sup> Návrh rozhodnutí, příloha I oddíl II bod 7 a oddíl III bod 11 a příloha I k uvedenému příloze.

<sup>71</sup> Návrh rozhodnutí, 64. bod odůvodnění.

„účinné správní a soudní ochrany pro subjekty údajů, jejichž osobní údaje se předávají“<sup>72</sup>. Tento požadavek připomíná i referenční rámec GDPR pro odpovídající ochranu<sup>73</sup>.

74. EDPB konstatuje, že tyto nápravné mechanismy jsou stejné jako mechanismy obsažené v bývalém štítu na ochranu soukromí, který byl předmětem připomínek pracovní skupiny zřízené podle článku 29<sup>74</sup>.
75. Pokud jde o rozhodčí mechanismus, EDPB konstatuje, že tato možnost není ve vztahu k výjimkám ze zásad rámce pro ochranu údajů<sup>75</sup> k dispozici, a proto odkazuje na svou připomínku uvedenou v bodě 33.
76. Pokud jde o další možnosti soudní nápravy, které jsou k dispozici podle práva USA, EDPB by rovněž uvítal další podrobnosti o uvedených právních předpisech<sup>76</sup> a odkázal na svou připomínku uvedenou v bodě 21.
77. EDPB dále vítá dopis FTC, která v něm popisuje svůj záměr úzce spolupracovat s orgány EU pro ochranu údajů<sup>77</sup>. EDPB rovněž vítá prioritizaci stížností ze strany FTC, ačkoli to subjektu údajů neposkytuje jistotu, že jeho stížnosti budou ve všech případech vyřízeny.
78. Pokud jde o možnost, aby fyzické osoby v určitých případech předkládaly své stížnosti některému z orgánů EU pro ochranu údajů, uvítal by EDPB další informace i) o tom, zda by možnost orgánu EU pro ochranu údajů poskytovat poradenství ohledně opatření vedoucích k nápravě nebo odškodnění mohla zahrnovat i doporučení ohledně pokut nebo využití vyšetřovacích pravomocí, a ii) o tom, do jaké míry by FTC nebo ministerstvo dopravy zohlednily opatření orgánu EU pro ochranu údajů jako důkaz pro opatření za účelem vymáhání práva<sup>78</sup>.
79. EDPB bude úzce monitorovat účinnost nápravných mechanismů, a to i v souvislosti s pravidelnými přezkumy.

### 3 PŘÍSTUP K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM Z EVROPSKÉ UNIE A JEJICH POUŽITÍ ORGÁNY VEŘEJNÉ MOCI V USA

#### 3.1 Přístup k osobním údajům a jejich použití pro účely prosazování trestního práva

##### 3.1.1 Přístup donucovacích orgánů k osobním údajům by měl být založen na jasných, přesných a přístupných pravidlech

80. EDPB vítá podrobnější informace a vysvětlení v porovnání s předchozím rozhodnutím o odpovídající ochraně, uvedené v návrhu rozhodnutí, pokud jde o přístup k osobním údajům a jejich používání orgány veřejné moci USA pro účely prosazování trestního práva. Návrh rozhodnutí obsahuje v příloze VI také dopis trestněprávní divize Ministerstva spravedlnosti USA, který „poskytuje krátký přehled primárních vyšetřovacích nástrojů využívaných pro získávání obchodních údajů a dalších informací ze

---

<sup>72</sup> Viz rovněž 141. bod odůvodnění GDPR odkazující na článek 47 Listiny základních práv obsahující právo na účinnou soudní ochranu v EU.

<sup>73</sup> Referenční rámec GDPR pro odpovídající ochranu, s. 8.

<sup>74</sup> Viz zejména stanovisko skupiny WP 29 č. 1/2016, oddíl 2.2.6 písm. a).

<sup>75</sup> Návrh rozhodnutí, příloha I přílohy I oddíl A.

<sup>76</sup> Návrh rozhodnutí, 85. bod odůvodnění.

<sup>77</sup> Návrh rozhodnutí, příloha IV.

<sup>78</sup> Návrh rozhodnutí, příloha I oddíl III bod 5 písm. b) podbod iii).

záznamů od společností v USA pro účely prosazování trestního práva nebo veřejného zájmu (občanského a regulačního), včetně omezení přístupu stanovených v těchto oprávněních“. Podle tohoto dopisu jsou všechny zákonné postupy popsané v tomto dopise využívány k získávání informací od společností v USA bez ohledu na státní příslušnost nebo místo bydliště subjektu údajů, a vyplývají buď přímo z Ústavy USA (čtvrtého dodatku), ze zákonných a procesních předpisů nebo z pokynů a postupů Ministerstva spravedlnosti USA. Tento přehled se nezabývá vyšetřovacími nástroji národní bezpečnosti využívanými donucovacími orgány při vyšetřování terorismu a při jiných vyšetřováních v oblasti národní bezpečnosti<sup>79</sup>.

81. EDPB konstatuje, že návrh rozhodnutí a jeho příloha VI se zabývají především federálními donucovacími a regulačními orgány<sup>80</sup> a neodkazují konkrétně na předpisy státního práva, které stanoví tyto postupy pro získávání informací. Příloha VI rovněž uvádí, že „podle specifických odvětví společností a typů údajů, které vlastní, existují ještě další právní základy k tomu, aby mohly společnosti napadnout žádosti vládních agentur o poskytnutí údajů“, přičemž navíc uvádí i několik ilustrativních příkladů, jako například zákon o bankovním tajemství (Bank Secrecy Act) a jeho prováděcí předpisy<sup>81</sup>, zákon o spravedlivém informování o úvěrové spolehlivosti (Fair Credit Reporting Act)<sup>82</sup> a zákon o právu na finanční soukromí (Right to Financial Privacy Act)<sup>83</sup>. EDPB konstatuje, že použitelný právní základ dané žádosti o přístup závisí na povaze požadovaných údajů, povaze společnosti, povaze právních postupů (trestních, správních, souvisejících s jiným veřejným zájmem) a povaze subjektu žádajícího o přístup. Vzhledem k tomu, že všechna platná pravidla pro omezení přístupu donucovacích orgánů k údajům předávaným do USA jsou založena na Ústavě Spojených států amerických, právních předpisech a transparentních politikách Ministerstva spravedlnosti USA, EDPB uznává dostupnost těchto pravidel a vyzývá Komisi, aby tento prvek v návrhu rozhodnutí zohlednila. Z přílohy VI vyplývá, že tyto zákony platí bez ohledu na státní příslušnost nebo místo bydliště subjektu údajů a obecně zahrnují požadavky čtvrtého dodatku (ačkoli často jdou nad rámec tohoto dodatku a zahrnují dodatečnou ochranu).
82. Závěrem EDPB konstatuje, že návrh rozhodnutí obsahuje podrobnější posouzení v porovnání s předchozím rozhodnutím o odpovídající ochraně, pokud jde o přístup federálních donucovacích orgánů. Pokud jde o přístup státních donucovacích orgánů, EDPB rovněž bere na vědomí, že podle přílohy VI musí být ochrana podle státního práva minimálně na stejné úrovni jako ochrana podle Ústavy USA, mimo jiné včetně čtvrtého dodatku. EDPB vyzývá Komisi, aby při budoucích přezkumech dále posuzovala prvek ochrany podle státního práva.

### 3.1.2 Nutnost prokázat nezbytnost a přiměřenost s ohledem na sledované legitimní cíle

83. EDPB řádně bere na vědomí, že žádost o přístup k údajům pro účely vymáhání práva lze obecně považovat za sledování legitimního cíle. Zároveň jsou však takové zásahy přijatelné pouze tehdy, jsou-li nezbytné a přiměřené<sup>84</sup>.

---

<sup>79</sup> Návrh rozhodnutí, poznámka pod čarou 1 v příloze VI.

<sup>80</sup> Viz návrh rozhodnutí, 90.–93. bod odůvodnění.

<sup>81</sup> Hlava 31 U.S.C. § 5318; hlava 31 Sbírký federálních předpisů (C.F.R.) kapitola X.

<sup>82</sup> Hlava 15 U.S.C. § 1681b.

<sup>83</sup> Hlava 12 U.S.C. § 3401–3423.

<sup>84</sup> Viz rozsudek Soudního dvora ze dne 6. října 2020 ve spojených věcech C-511/18, C-512/18 a C-520/18, La Quadrature du Net a další, ECLI:EU:C:2020:791 (dále jen „rozsudek SDEU ve věci La Quadrature du Net“), bod 140. Viz rovněž Evropský inspektor ochrany údajů, [Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit](#) (Posouzení nezbytnosti opatření, která omezují

84. Zásada přiměřenosti podle ustálené judikatury SDEU vyžaduje, aby legislativní opatření představující zásahy do práva na soukromý život a na ochranu osobních údajů byla způsobilá „k uskutečnění legitimních cílů sledovaných dotčenou právní úpravou“ a aby nepřekračovala „meze toho, co je přiměřené a nezbytné k dosažení těchto cílů“<sup>85</sup>. Posouzení nezbytnosti a přiměřenosti se tedy v zásadě vždy provádí ve vztahu ke konkrétnímu opatření stanovenému právními předpisy.
85. Orgány USA v příloze VI specifikují, že federální státní zástupci a federální vyšetřovatelé mohou získat přístup k dokumentům a dalším informacím ze záznamů od organizací prostřednictvím „několika typů povinných zákonných postupů, včetně předvolání velkou porotou, správních předvolání a příkazů k prohlídce“, a mohou získat další komunikaci „v rámci federálních pravomocí odposlechu telefonních rozhovorů a získávání informací ze zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení (pen registers)“<sup>86</sup>. Agentury s občanskými a regulačními úkoly navíc mohou vydávat předvolání pro organizace k předložení „obchodních záznamů, elektronicky uložených informací nebo jiných hmotných předmětů“<sup>87</sup>. Samotné tyto procesy jsou vysvětleny rovněž v 90.–93. bodě odůvodnění návrhu rozhodnutí. EDPB v tomto ohledu konstatuje pozitivní vývoj uvedený v návrhu rozhodnutí v judikatuře USA, pokud jde o elektronicky uchovávané informace<sup>88</sup>.
86. Příloha VI dále upřesňuje, že tyto zákonné postupy jsou nediskriminační a jsou zpravidla využívány k získávání informací od „společností“ v USA bez ohledu na to, zda jsou certifikovány v rámci EU-USA pro ochranu údajů a „bez ohledu na státní příslušnost či bydliště subjektu údajů“.
87. Příloha VI navíc obsahuje zjištění týkající se záruk podle čtvrtého dodatku Ústavy USA, podle něhož je pro účel domovní prohlídky a zabavení ze strany donucovacích orgánů především požadován soudní příkaz vystavený na základě prokázání důvodného podezření, a odkazuje na skutečnost, že ve výjimečných případech, kdy se na danou situaci požadavek soudního příkazu nevztahuje, podléhá vymáhání práva zkoušce „přiměřenosti“ podle čtvrtého dodatku<sup>89</sup>. Osoba, která je předmětem prohlídky nebo jejíž majetek je předmětem prohlídky, může usilovat o to, aby byly prohlášeny za neplatné důkazy získané při nezákonné prohlídce nebo z této prohlídky odvozené, pokud jsou tyto důkazy použity proti této osobě během trestního řízení<sup>90</sup>.
88. Závěrem EDPB konstatuje, že systém vyšetřovacích nástrojů používaných k získávání obchodních údajů a jiných informací o záznamech od společností v USA pro účely prosazování trestního práva nebo

---

základní právo na ochranu osobních údajů: nástroje), 11. dubna 2017 a Evropský inspektor ochrany údajů, [Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data](#) (Pokyny k posuzování přiměřenosti opatření omezujících základní právo na soukromí a na ochranu osobních údajů), 19. prosince 2019.

<sup>85</sup> Viz rozsudek Soudního dvora ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238 (dále jen „rozsudek SDEU ve věci Digital Rights Ireland“), bod 46 a citovaná judikatura.

<sup>86</sup> Návrh rozhodnutí, příloha VI, s. 2.

<sup>87</sup> Návrh rozhodnutí, příloha VI, s. 4.

<sup>88</sup> Viz návrh rozhodnutí, poznámka pod čarou 146. Nejvyšší soud USA v rozsudku z roku 2018 potvrdil, že příkaz k prohlídce nebo výjimka z příkazu se vyžaduje rovněž pro přístup donucovacích orgánů k historickým záznamům vysílačů, které poskytují komplexní přehled o pohybech uživatele, a že uživatel může odůvodněně očekávat zachování soukromí s ohledem na tyto informace (Timothy Ivory Carpenter v. United States of America, č. 16-402, 585 U.S. (2018)).

<sup>89</sup> Viz návrh rozhodnutí, příloha VI, s. 2.

<sup>90</sup> Viz návrh rozhodnutí, 90. bod odůvodnění.



veřejného zájmu – včetně omezení přístupu a záruk – poskytuje komplexní, ale také složitý systém opatření, který mimo jiné odráží federální povahu vlády USA.

89. Bylo by tak možné mít za to, že systém vyšetřovacích opatření využívaných donucovacími orgány v USA obecně splňuje požadavky nezbytnosti a přiměřenosti ve vztahu k základním právům na soukromý život a ochranu údajů.

### 3.1.3 Měl by existovat mechanismus nezávislého dohledu

90. EDPB bere na vědomí skutečnost, že většina postupů popsaných v návrhu rozhodnutí a v příloze VI předpokládá existenci soudního rozhodnutí dříve, než orgány získají přístup k údajům (např. soudní příkazy týkající se zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení (pen register) nebo zařízení pro zaznamenávání informací o příchozí komunikaci sledovaného zařízení (trap and trace)<sup>91</sup>, soudní nařízení sledování podle federálního zákona o odposlechu (Federal Wiretap Law)<sup>92</sup>, příkazy k prohlídce podle federálního trestního řádu (Federal Rules of Criminal Procedure), pravidlo 41<sup>93</sup>). Zdá se však, že ne všechny vyžadují *a priori* účast soudu. „Vydávat předvolání“ mohou například i občanské a regulační orgány<sup>94</sup>. V těchto případech však existuje možnost následné soudní kontroly odůvodněnosti tohoto předvolání, neboť „adresát správního předvolání může napadnout výkon předvolání u soudu“<sup>95</sup>.
91. Návrh rozhodnutí navíc popisuje dohled nad federálními donucovacími orgány činnými v trestním řízení prováděný různými orgány, od vnitřní kontroly ze strany úředníků pro ochranu údajů a občanských svobod až po vnější kontrolu prováděnou generálním inspektorem a zvláštními výbory v Kongresu USA<sup>96</sup>. Evropská komise poskytuje podrobné a diferencované informace a zpravidla dochází ke srozumitelným závěrům. EDPB proto v tomto stanovisku upustil od opakování faktických zjištění a hodnocení.
92. EDPB na základě dostupných informací konstatuje, že pokud jde o přístup donucovacích orgánů k údajům v držení společností v USA, je zaveden poměrně spolehlivý mechanismus nezávislého dohledu.

### 3.1.4 Fyzické osoby musí mít k dispozici účinné prostředky nápravy

93. Podle judikatury SDEU musí mít fyzické osoby k dispozici účinný prostředek nápravy, aby uspokojily svá práva, pokud se domnívají, že nejsou nebo nebyla respektována. SDEU v rozsudku ve věci Schrems I objasnil, že „právní úprava, která nestanoví procesním subjektům žádnou možnost využít právních prostředků s cílem získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu těchto údajů, nerespektuje podstatu základního práva na účinnou právní ochranu zakotveného v článku 47 Listiny. Článek 47 první pododstavec Listiny totiž vyžaduje, aby každý, jehož práva a svobody zaručené právem Unie byly porušeny, měl za podmínek stanovených tímto článkem právo na účinné prostředky nápravy před soudem.“<sup>97</sup>

---

<sup>91</sup> Viz návrh rozhodnutí, 92. bod odůvodnění.

<sup>92</sup> Viz návrh rozhodnutí, příloha VI, s. 3.

<sup>93</sup> Viz návrh rozhodnutí, 90. bod odůvodnění a příloha VI, s. 3.

<sup>94</sup> Viz návrh rozhodnutí, příloha VI, s. 4, a 91. bod odůvodnění.

<sup>95</sup> Viz návrh rozhodnutí, příloha VI, s. 4, a 91. bod odůvodnění.

<sup>96</sup> Viz návrh rozhodnutí, 103.–106. bod odůvodnění.

<sup>97</sup> Rozsudek SDEU ve věci Schrems I, bod 95.

94. Návrh rozhodnutí<sup>98</sup> a jeho příloha VI obsahují další informace týkající se možných opravných prostředků vyplývajících z právních předpisů, které by byly k dispozici fyzickým osobám, pokud by orgány veřejné moci neoprávněně získaly přístup k jejich údajům.
95. V tomto ohledu podle Komise<sup>99</sup> hlava 5 U.S.C. § 702 (zákon o správním řízení (Administrative Procedure Act, APA)) stanoví, že kdokoli, jemuž krok agentury způsobí právní krivdu nebo kdo je krokem agentury ve smyslu příslušného zákona negativně postižen nebo poškozen, má právo domáhat se jeho soudního přezkumu.
96. Zákon o uchovávaných komunikacích (Stored Communications Act, SCA) (přijatý jako hlava II zákona o soukromí elektronických komunikací (Electronic Communications Privacy Act)) dále stanoví, že kdokoli, kdo je poškozen jakýmkoli porušením uvedené kapitoly, pokud k tomuto porušení došlo v důsledku vědomého nebo úmyslného jednání, může v občanskoprávním řízení požadovat od osoby nebo subjektu jiného než Spojené státy, který se tohoto porušení dopustil, přiměřenou nápravu<sup>100</sup>. Kromě toho může kdokoli, kdo je poškozen jakýmkoli úmyslným porušením uvedené kapitoly nebo kapitoly 119, podat žalobu u okresního soudu USA proti Spojeným státům americkým za účelem získání peněžité náhrady škody<sup>101</sup>.
97. Návrh rozhodnutí navíc obsahuje informace o právu získat přístup k záznamům federálních agentur podle zákona o svobodě informací (Freedom of Information Act, FOIA)<sup>102</sup> a několika dalších zákonů, které dávají fyzickým osobám právo žalovat orgán veřejné moci USA nebo úředníka, pokud jde o zpracování osobních údajů, například zákon o odposleších (Wiretap Act), zákon o počítačových podvodech a zneužití počítače (Computer Fraud and Abuse Act), zákon o deliktních žalobách u federálního soudu (Federal Torts Claim Act), zákon o právu na finanční soukromí (Right to Financial Privacy Act) a zákon o spravedlivém informování o úvěrové spolehlivosti (Fair Credit Reporting Act)<sup>103</sup>.
98. EDPB proto vítá vysvětlení, které Komise poskytla, pokud jde o počet právních možností nápravy, které mají fyzické osoby k dispozici. EDPB rovněž vyzývá Komisi, aby dále objasnila, zda tyto opravné prostředky umožňují subjektu údajů „získat přístup k osobním údajům, které se ho týkají, nebo dosáhnout opravy či výmazu těchto údajů“, jak požaduje SDEU.

### 3.1.5 Další využití shromážděných informací

#### 3.1.5.1 Další využití předávaných údajů, ke kterým mají přístup donucovací orgány, v rámci USA

99. EDPB vnímá příznivě, že návrh rozhodnutí posuzuje další využívání údajů, k nimž mají přístup donucovací orgány v rámci USA. EDPB však lituje, že je uveden pouze jeden příklad důvodů, na jejichž základě mohou být tyto informace dále šířeny<sup>104</sup>. EDPB v tomto ohledu doporučuje Komisi, aby do návrhu rozhodnutí zahrнула další objasnění zásad a záruk platných pro další využívání údajů, jako jsou například zásady a záruky obsažené v zákoně o ochraně soukromí (Privacy Act, hlava 5 U.S.C. § 552a)<sup>105</sup>.

<sup>98</sup> Viz návrh rozhodnutí, 107. až 112. bod odůvodnění.

<sup>99</sup> Viz návrh rozhodnutí, 109. bod odůvodnění.

<sup>100</sup> Hlava 18 U.S.C. § 2707.

<sup>101</sup> Hlava 18 U.S.C. § 2712.

<sup>102</sup> Viz návrh rozhodnutí, 111. bod odůvodnění.

<sup>103</sup> Viz návrh rozhodnutí, 112. bod odůvodnění.

<sup>104</sup> Viz návrh rozhodnutí, 102. bod odůvodnění.

<sup>105</sup> Viz pokyny ministra spravedlnosti pro domácí operace FBI (Attorney General Guidelines for Domestic FBI Operations, AGG-DOM), s. 36, oddíl B bod 1 písm. g).

### 3.1.5.2 Další předávání mimo USA

100. EDPB dále konstatuje, že Evropská komise poukázala rovněž na další předávání údajů donucovacími orgány v USA orgánům ve třetích zemích, ale opět pouze s ohledem na pokyny ministra spravedlnosti pro domácí operace FBI (AGG-DOM)<sup>106</sup>. EDPB se domnívá, že takové informace a hodnocení jsou klíčové, aby bylo možné provést komplexní posouzení úrovně ochrany poskytované právním rámcem USA a jeho postupů, které se týkají zpřístupnění a dalšího použití údajů v zahraničí. Vzhledem k tomu, že Komise uvedla pouze jeden omezený příklad týkající se otázky dalšího předávání mimo USA jako celku, vyzývá EDPB Komisi, aby dále objasnila platná pravidla a záruky pro další předávání, další používání a zpřístupňování osobních informací shromážděných pro účely vymáhání práva v USA a následně předávaných do třetích zemí, mimo jiné prostřednictvím mezinárodních dohod.

## 3.2 Přístup a použití pro účely národní bezpečnosti

101. Obecně EDPB podotýká, že jsou státům v záležitostech národní bezpečnosti ponechány široké posuzovací pravomoci, což uznává i ESLP. EDPB rovněž připomíná, že jak je zdůrazněno v jeho aktualizovaném doporučení týkajícím se evropských základních záruk pro sledovací opatření<sup>107</sup>, čl. 6 odst. 3 Smlouvy o Evropské unii stanoví, že základní práva zakotvená 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<sup>108</sup>. Úroveň ochrany základních práv vyžadovaná v článku 45 GDPR musí být určena na základě ustanovení uvedeného nařízení ve spojení se základními právy zaručenými Listinou základních práv EU. V tomto ohledu mají podle čl. 52 odst. 3 Listiny 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, tudíž musí být zohledněna jako minimální úroveň ochrany pro výklad odpovídajících práv v Listině<sup>109</sup>. Podle poslední věty čl. 52. odst. 3 Listiny to však „[n]ebrání tomu, aby právo Unie poskytovalo širší ochranu“.
102. V následujícím posouzení tudíž EDPB zohlednil judikaturu ESLP v tom smyslu, že Listina, tak jak ji vykládá SDEU, nestanoví vyšší úroveň ochrany ukládající jiné požadavky než judikatura ESLP.
103. V právním rámci USA existuje několik právních nástrojů, které poskytují zpravodajským službám USA možnost shromažďovat údaje a dále k nim přistupovat a zpracovávat je.
104. Jak připomněla Evropská komise ve svém návrhu rozhodnutí, „zpravodajské služby USA se mohou domáhat přístupu k osobním údajům, které byly předány organizacím se sídlem v USA pro účely národní bezpečnosti, pouze na základě zákona, konkrétně podle zákona o dohledu nad zahraniční informační službou (FISA), nebo zákonných ustanovení umožňujících přístup prostřednictvím tzv. National Security Letters (NSL)“<sup>110</sup>. „Zpravodajské služby mají rovněž možnost shromažďovat osobní údaje mimo USA, což může zahrnovat osobní údaje na cestě mezi Uníí a USA“ podle prezidentského dekretu 12333 (EO 12333)<sup>111</sup>.

<sup>106</sup> Viz návrh rozhodnutí, 102. bod odůvodnění.

<sup>107</sup> Viz doporučení EDPB 2/2020 týkající se evropských základních záruk pro sledovací opatření.

<sup>108</sup> Viz rozsudek SDEU ve věci Schrems II, bod 98.

<sup>109</sup> Viz rozsudek SDEU ve věci La Quadrature du Net, bod 124.

<sup>110</sup> Viz návrh rozhodnutí, 115. bod odůvodnění.

<sup>111</sup> Viz návrh rozhodnutí, 117. bod odůvodnění.

105. Pokud jde o konkrétní režimy shromažďování údajů, zejména § 702 zákona FISA a dekret EO 12333, dekret EO 14086 nyní stanoví nová pravidla pro posílení záruk pro činnosti signálového zpravodajství USA. Tato obecná pravidla platí horizontálně a „*musí být dále implementována prostřednictvím politik a postupů agentur, které je transponují do konkrétních pokynů pro každodenní operace*“<sup>112</sup>. Dekret EO 14086 z větší části nahradil předchozí prezidentskou politickou směrnicí (Presidential Policy Directive) č. 28 (dále jen „PPD-28“)<sup>113</sup>.
106. Pro posouzení právního rámce vztahujícího se na shromažďování údajů pro účely národní bezpečnosti, přístup k nim a jejich další zpracování je proto důležité přezkoumat konkrétní právní rámec upravující shromažďování údajů v USA i mimo ně, tj. § 702 zákona FISA a dekret EO 12333, které se jako takové od předchozího přezkumu štítu na ochranu soukromí nezměnily, s přihlédnutím ke skutečnosti, že nový dekret EO 14086 poskytuje záruky, které mají být zavedeny také v souvislosti se shromažďováním údajů na základě konkrétních právních předpisů, jako je § 702 zákona FISA a EO 12333.

### 3.2.1 Záruka A – Zpracování by mělo být v souladu se zákonem a mělo by být založeno na jasných, přesných a přístupných pravidlech

107. EDPB chce ohledně posouzení obecného uspořádání shromažďování údajů pro účely národní bezpečnosti připomenout první ze čtyř takzvaných „evropských základních záruk“, která zní, že „zpracování údajů by se mělo zakládat na jasných, přesných a přístupných pravidlech“<sup>114</sup>.
108. V souladu s ustálenou judikaturou SDEU musí být každé omezení práva na ochranu osobních údajů stanoveno zákonem a právní základ dovolující zásah do těchto práv musí sám definovat rozsah omezení výkonu dotyčného práva<sup>115</sup>. Soudní dvůr navíc připomněl, že „právní úprava musí být právně závazná ve vnitrostátním právu“<sup>116</sup>. V tomto ohledu judikatura ESLP upřesňuje, že pojem „právo“ je třeba chápat v jeho věcném, nikoli formálním smyslu. Může zahrnovat podzákonné předpisy a regulační akty přijaté profesními regulačními orgány v rámci nezávislých zákonodárných pravomocí, které na ně delegoval parlament, a dokonce i nepsané právo. Aby byla norma „právem“, musí být přinejmenším přiměřeně přístupná a musí být formulována s dostatečnou přesností<sup>117</sup>.
109. Požadovaný stupeň přesnosti je nutno posuzovat ve vztahu k rozsahu daného omezení práva<sup>118</sup>. Kromě toho, pokud jde o „předvídatelnost“ zákona, ESLP v rozsudku ve věci Zakharov připomněl, že v kontextu utajovaných opatření v oblasti sledování, jako je například odposlouchávání komunikace, „předvídatelnost neznamená, že by jednotlivec měl být s to předvídat, kdy je pravděpodobné, že orgány zachytí jeho komunikaci, aby tomu mohl přizpůsobit své chování“. Jsou však nezbytná jasná a podrobná pravidla pro utajovaná opatření v oblasti sledování, aby se předešlo riziku svévolných zásahů

<sup>112</sup> Viz návrh rozhodnutí, 120. bod odůvodnění.

<sup>113</sup> Tento dekret ruší směrnici PPD-28 s výjimkou oddílů 3 a 6 a utajované přílohy této směrnice, které zůstávají v platnosti. Viz prezidentské memorandum o národní bezpečnosti ze dne 7. října 2022.

<sup>114</sup> Doporučení 2/2020 týkající se evropských základních záruk pro sledovací opatření, přijaté dne 10. listopadu 2020. Viz body 175 a 180 rozsudku ve věci Schrems II a stanovisko č. 1/15 (dohoda mezi EU a Kanadou o jmenné evidenci cestujících) ze dne 26. července 2017, bod 139 a citovaná judikatura.

<sup>115</sup> Viz rozsudek SDEU ve věci Schrems II, body 174–175 a citovaná judikatura. Pokud jde o přístup orgánů veřejné moci členských států, viz rovněž věc C-623/17 Privacy International, ECLI:EU:C:2020:790 (dále jen „rozsudek SDEU ve věci Privacy International“), bod 65, a rozsudek SDEU ve věci La Quadrature du Net, bod 175.

<sup>116</sup> Rozsudek SDEU ve věci Privacy International, bod 68.

<sup>117</sup> ESLP, rozsudek ve věci Sunday Times v. Spojené království (č. 1) ze dne 26. dubna 1979, CE:ECHR:1979:0426JUD000653874 (dále jen „rozsudek ESLP ve věci Sunday Times v. Spojené království č. 1“), bod 49.

<sup>118</sup> Rozsudek ESLP ve věci Sunday Times v. Spojené království č. 1, bod 49.

v případech, kdy je pravomoc svěřená výkonné moci vykonávána tajně. „Vnitrostátní právo však musí být dostatečně jasné na to, aby poskytlo občanům odpovídající představu o okolnostech a podmínkách, za jakých se mohou orgány veřejné moci k užití jakýchkoli takových opatření uchýlit“<sup>119</sup>.

110. SDEU dále objasnil, že posouzení použitelného práva třetí země by se mělo zaměřit na to, zda se ho mohou jednotlivci dovolávat a domáhat se ho před soudem. Práva přiznaná subjektům údajů by měla být zejména vymahatelná, a fyzickým osobám musí být poskytnuta vymahatelná práva vůči orgánům veřejné moci<sup>120</sup>, která v kontextu předchozí směrnice PPD-28 poskytnuta nebyla. Dekret EO 14086, který má podle informací EDPB v rámci právního řádu USA stejný právní účinek jako směrnice PPD-28 (tj. je závazný pro výkonnou moc), nyní stanoví vymahatelné nároky vůči orgánům veřejné moci. Podrobné posouzení těchto nových vymahatelných práv subjektů údajů je uvedeno v oddíle o nápravných opatřeních.
111. Ve 114. až 152. bodě odůvodnění návrhu rozhodnutí a příloze VII jsou shrnuty některé aspekty platného právního rámce, omezení shromažďování informací, omezení uchovávání a šíření informací, soulad s předpisy a dohled, transparentnost a nápravná opatření. Právní systém USA pro zpravodajské činnosti se skládá z řady různých dokumentů včetně zpráv jednotlivých agentur, politik a postupů. V tomto ohledu se hodnocení EDPB zaměřuje na omezený počet otázek, které považuje za zásadní.
112. Podle 115. až 119. bodu odůvodnění návrhu rozhodnutí mohou mít vnitrostátní bezpečnostní orgány USA přístup k předaným osobním údajům pouze na základě zákona FISA, jiných zákonných ustanovení (hlava 12 U.S.C. § 3414, hlava 15 U.S.C. § 1681u–1681v a hlava 18 U.S.C. § 2709) nebo v souvislosti s osobními údaji na cestě na základě dekretu EO 12333. Z 116. a 118. bodu odůvodnění návrhu rozhodnutí vyplývá, že se Komise ve svém posouzení v souvislosti s přístupem vnitrostátních bezpečnostních orgánů USA k osobním údajům zaměřuje na § 105, 302, 402, 501 a 702 zákona FISA (zahraniční zpravodajská činnost zaměřená na osoby, které nejsou občany USA a nacházejí se mimo USA) a na dekret EO 12333 (zahraniční zpravodajská činnost týkající se osobních údajů na cestě) vzhledem k tomu, že jsou nejrelevantnější. Stanovisko EDPB je proto omezeno na posouzení těchto ustanovení Komise s přihlédnutím k omezením a zárukám stanoveným v dekretu EO 14086<sup>121</sup>.
113. V tomto ohledu je třeba poznamenat, že všechny právní nástroje uvedené v návrhu nařízení jsou přístupné široké veřejnosti (v USA i mimo ně) a dostupné online. Požadavky stanovené v dekretu EO jsou navíc závazné pro celou zpravodajskou komunitu<sup>122</sup> a vztahují se průřezově na všechny činnosti prováděné pro účely zahraničních zpravodajských informací.
114. Pojem „signálové zpravodajství“ není v dekretu EO 14086 definován. Dekret EO 14086 odkazuje na definice uvedené v dekretu EO 12333 pro stanovení oblasti působnosti zahraničního zpravodajství a kontrarozvědky, které jsou zde vymezeny jen široce. V tomto ohledu, i když byl vznesen argument, že od zavedení zákona FISA lze dekret EO 12333 uplatňovat pouze pro shromažďování údajů mimo území USA, EDPB připomíná, že samotný dekret EO 12333, který zůstává beze změny, neobsahuje dostatečně podrobné informace týkající se jeho zeměpisné oblasti působnosti, rozsahu, v jakém mohou být údaje shromažďovány, uchovávány nebo dále šířeny, ani o povaze trestných činů, které mohou vést ke sledování, či o druhu informací, které mohou být shromažďovány nebo používány. V zásadě může

---

<sup>119</sup> Rozsudek ESLP ve věci Zakharov v. Rusko ze dne 4. prosince 2015 (dále jen „rozsudek ESLP ve věci Zakharov“), bod 229.

<sup>120</sup> Rozsudek SDEU ve věci Schrems II, bod 181.

<sup>121</sup> Tento dekret ruší směrnici PPD-28 s výjimkou oddílů 3 a 6 a utajované přílohy této směrnice, které zůstávají v platnosti. Viz [prezidentské memorandum o národní bezpečnosti ze dne 7. října 2022](#).

<sup>122</sup> Viz návrh rozhodnutí, 120. bod odůvodnění.

veškeré shromažďování zahraničních zpravodajských informací v působnosti dekretu EO 12333 probíhat podle uvážení prezidenta USA<sup>123</sup>. Podle názoru EDPB je však hlavním účelem dekretu EO 14086 stanovit omezení pro shromažďování a zpracování osobních údajů v souvislosti se zahraničním zpravodajstvím bez ohledu na to, jaký program sledování je použit a odkud jsou údaje získávány. EDPB má proto za to, že dodatečné záruky stanovené v dekretu EO 14086 se použijí také v souvislosti s programy sledování použitelnými na osobní údaje na cestě, které se provádějí v souladu s dekretem EO 12333<sup>124</sup>.

115. V tomto ohledu uvádí dekret EO 14086 dvanáct legitimních cílů, které by měly být sledovány při shromažďování informací v rámci signálového zpravodajství, a pět cílů, u nichž shromažďování informací v rámci signálového zpravodajství prováděno být nesmí<sup>125</sup> jakož i šest legitimních cílů pro hromadné shromažďování údajů<sup>126</sup>. Zatímco některé z nich jsou poměrně podrobné (např. „záchrana rukojmích“), jiné jsou obecnější (např. „globální bezpečnost“). Dekret EO 14086 rovněž uvádí seznam zakázaných cílů, který zahrnuje zejména potlačení nebo omezení „oprávněných zájmů v oblasti soukromí“<sup>127</sup>. Dekret EO 14086 rovněž stanoví možnost, aby prezident USA doplnil na seznam informací, jejichž shromažďování je povoleno, i další cíle, které by na základě rozhodnutí prezidenta nemusely být zveřejněny, pokud se prezident domnívá, že by to představovalo riziko pro národní bezpečnost USA<sup>128</sup>. Tyto aktualizace mohou být povoleny pouze „s ohledem na nové požadavky národní bezpečnosti“.
116. Není možné, aby zpravodajské agentury odůvodňovaly shromažďování informací prostřednictvím signálového zpravodajství pouze na základě cílů jako takových, ale musí je pro operativní účely dále doložit konkrétnějšími prioritami, které mohou být důvodem pro toto shromažďování. Dekret EO 14086 podrobně popisuje postup ověřování priorit, které mohou být důvodem pro shromažďování informací prostřednictvím signálového zpravodajství<sup>129</sup>. EDPB chápe, že proces definování uznaných zpravodajských priorit v zásadě závisí na řediteli zpravodajských služeb, a uznává, že by měl zpravidla zahrnovat posouzení úředníka pro ochranu občanských svobod z Úřadu ředitele národních zpravodajských služeb (CLPO), s nímž ředitel může nesouhlasit, a v takovém případě „při předkládání rámce národních zpravodajských priorit (National Intelligence Priorities Framework, NIPF) prezidentovi zahrne i posouzení CLPO a názory ředitele“<sup>130</sup>.
117. EDPB však také konstatuje, že podle definice „uznané zpravodajské priority“ se takovými prioritami rozumí „většina činností USA v oblasti shromažďování informací prostřednictvím signálového zpravodajství“<sup>131</sup>, které jsou uznanou prioritou podle § 2 písm. b) bodu iii) uvedeného dekretu (jak je popsáno v předchozím odstavci). Proces ověřování se může v některých případech od tohoto procesu lišit v „úzce vymezených případech“; v takovém případě může prezident nebo vedoucí daného prvku zpravodajské služby stanovit prioritu „v proveditelném rozsahu“ v souladu s kritérii stanovenými

---

<sup>123</sup> Podle článku II Ústavy USA spadá odpovědnost za zajištění národní bezpečnosti, zahrnující zejména shromažďování zahraničních zpravodajských informací, do pravomoci prezidenta jakožto vrchního velitele ozbrojených sil.

<sup>124</sup> Viz návrh rozhodnutí, 134. bod odůvodnění.

<sup>125</sup> Viz dekret EO 14086, § 2(b)(ii)(A), body 1 až 5.

<sup>126</sup> Viz návrh rozhodnutí, 134. bod odůvodnění, a dekret EO 14086, § 2(c)(ii).

<sup>127</sup> Viz EO 14086, § 2(b)(ii)(A)(2).

<sup>128</sup> Viz EO 14086, § 2(b)(i)(B).

<sup>129</sup> Viz návrh rozhodnutí, 129. bod odůvodnění.

<sup>130</sup> Viz EO 14086, § 2(b)(iii)(B).

<sup>131</sup> Viz EO 14086, § 4(n).

v témže § 2(b)(iii)(A)(1)–(3), která zahrnuje požadavek náležitého zohlednění soukromí a občanských svobod všech osob, avšak bez účasti CLPO.

118. Dekret EO 14086 navíc zdůrazňuje, že „shromažďování informací prostřednictvím signálového zpravodajství musí být v nejvyšší možné míře individuálně uzpůsobeno“ za účelem prosazování uznané zpravodajské priority, a že „zpravodajská služba zváží dostupnost, proveditelnost a vhodnost jiných, méně obtěžujících zdrojů“ a stanoví obecné požadavky na nezbytnost a přiměřenost<sup>132</sup>.
119. Kromě toho dekret EO 14086 podle § 5 písm. h) zakládá nárok na předkládání způsobilých stížností CLPO a dosažení toho, aby rozhodnutí CLPO bylo přezkoumáno odvolacím soudem pro ochranu údajů v souladu s nápravným mechanismem stanoveným v § 3 uvedeného dekretu.
120. Text zákona FISA se jeví jako jasnější a přesnější než dekret EO 12333, pokud jde o druh zpravodajských operací, které mohou být vyžadovány. Zákon FISA a dekret EO 12333 musí být nyní uplatňovány s ohledem na dekret EO 14086, a to zejména s přihlédnutím k zásadám nezbytnosti a přiměřenosti.
121. Požadavky stanovené v dekretu EO 14086 musí být dále prováděny prostřednictvím politik a postupů jednotlivých zpravodajských agentur, které je transponují do konkrétních pokynů pro každodenní operace. V tomto ohledu poskytuje dekret EO 14086 zpravodajským službám USA maximálně jeden rok na aktualizaci jejich stávajících politik a postupů (tj. do 7. října 2023), aby tak byly uvedeny do souladu s požadavky dekretu EO. Tyto aktualizované politiky a postupy musí být vypracovány po konzultaci s ministrem spravedlnosti, CLPO a Výborem pro dohled nad ochranou soukromí a občanských svobod (PCLOB) a musí být v maximální možné míře zpřístupněny veřejnosti<sup>133</sup>.
122. EDPB by uvítal, kdyby nejen vstup v platnost, ale i přijetí tohoto rozhodnutí byly podmíněny mimo jiné přijetím aktualizovaných politik a postupů k provádění dekretu EO 14086 všemi zpravodajskými službami USA. EDPB doporučuje Komisi, aby tyto aktualizované politiky a postupy posoudila a toto posouzení se sborem EDPB sdílela.
123. A konečně pokud jde o uchovávání předávaných údajů, které již byly shromážděny pro účely národní bezpečnosti, EDPB konstatuje, že dekret EO 14086 zajišťuje, aby se pravidla platná pro osobní údaje osob, které jsou občany USA, vztahovala i na osobní údaje osob, které nejsou občany USA<sup>134</sup>. Z návrhu rozhodnutí vyplývá, že tato pravidla jsou stanovena v § 309 zákona o povolení zpravodajské činnosti pro fiskální rok 2015 (Intelligence Authorization Act For Fiscal Year 2015<sup>135</sup>), který stanoví maximální dobu uchovávání jakékoli neveřejné telefonické nebo elektronické komunikace získané bez souhlasu dané osoby v zásadě na 5 let. EDPB v tomto ohledu doporučuje, aby Komise v rozhodnutí blíže objasnila své posouzení pravidel vztahujících se na uchovávání osobních údajů osob, které jsou občany USA.

### 3.2.2 Záruka B – Nutnost prokázat nezbytnost a přiměřenost s ohledem na sledované legitimní cíle

#### 3.2.2.1 Horizontální záruky stanovené novým dekretem 14086 – nezbytnost a přiměřenost

124. Cílem nového dekretu EO 14086, který obecně nahrazuje směrnici PPD-28, je poskytnout pravidla pro posílení záruk pro činnosti signálového zpravodajství USA, která mají být dále prováděna prvky zpravodajských služeb prostřednictvím jejich vnitřních politik a postupů.

---

<sup>132</sup> Viz EO 14086, § 2(c)(i)(A) a (B).

<sup>133</sup> Viz EO 14086, § 2(c)(iv)(B) a (C).

<sup>134</sup> Návrh rozhodnutí, 150. bod odůvodnění.

<sup>135</sup> Návrh rozhodnutí, poznámka pod čarou 272.

125. Dekret EO 14086 zavádí dva nové požadavky podle práva USA, které odrážejí požadavky připomenuté Soudním dvorem Evropské unie v rozsudku ve věci Schrems II, a sice, že činnosti signálového zpravodajství jsou prováděny pouze v rozsahu nezbytném pro shromažďování podle uznaných zpravodajských priorit a pouze v rozsahu a způsobem, který je přiměřený ve vztahu k těmto uznaným zpravodajským prioritám<sup>136</sup>.
126. EDPB má za to, že tyto prvky byly začleněny proto, aby odrážely zásady nezbytnosti a přiměřenosti stanovené v právu EU a v judikatuře SDEU a EÚLP, jejichž cílem je zajistit, aby shromažďování a zpracování údajů byly omezeny na to, co je nezbytné a přiměřené.
127. V této souvislosti EDPB připomíná postup předpokládaný pro uznávání zpravodajských priorit, jakož i možnou výjimku (viz body 116 a 117).
128. EDPB dále konstatuje, že tyto zásady nezbytnosti a přiměřenosti stanovené v dekretu EO budou muset být do jednoho roku uvedeny do praxe a zavedeny do politik a postupů jednotlivých prvků zpravodajských služeb<sup>137</sup>.

#### 3.2.2.2 Zvláštní záruky pro shromažďování informací prostřednictvím signálového zpravodajství

129. EDPB rovněž konstatuje, že dekret EO 14086 stanoví omezení týkající se cílů, pro něž lze a nelze shromažďovat osobní údaje v souvislosti se shromažďováním informací prostřednictvím signálového zpravodajství<sup>138</sup>.
130. EDPB vítá, že dekret EO stanoví, že cílené shromažďování by mělo mít přednost před hromadným shromažďováním<sup>139</sup>. S ohledem na shromažďování informací prostřednictvím signálového zpravodajství stanoví dekret EO seznam 12 cílů, pro něž je možno údaje shromažďovat a které je třeba dále doložit, aby mohly být považovány za zpravodajské priority (viz bod 117), jakož i 5 cílů, u nichž shromažďování informací prostřednictvím signálového zpravodajství prováděno být nesmí<sup>140</sup>. Tato ustanovení v zásadě představují záruku pro zajištění nezbytnosti shromažďování údajů.
131. EDPB však připomíná, že dekret EO 14086 rovněž stanoví možnost, aby prezident Spojených států doplnil na seznam další cíle (viz body 114 a 115)<sup>141</sup>.

#### 3.2.2.3 Zvláštní záruky pro hromadné shromažďování

132. SDEU ve svém rozsudku ve věci Schrems I zdůraznil, že „ochrana základního práva na respektování soukromého života na unijní úrovni vyžaduje, aby výjimky z ochrany osobních údajů a její omezení byly činěny v mezích toho, co je naprosto nezbytné“<sup>142</sup>, a rozhodl, že „právní úprava, která veřejným orgánům umožňuje globální přístup k obsahu elektronických komunikací, musí být považována za zasahující do podstaty základního práva na respektování soukromého života zaručeného článkem 7 Listiny“.
133. Soudní dvůr ve věci Schrems II<sup>143</sup> s ohledem na svou analýzu hromadného shromažďování ve vztahu k souvisejícímu výkladu dekretu EO 12 333 a směrnice PPD-28, a zejména bodů 183 až 185, zdůraznil,

<sup>136</sup> Viz EO 14086, § 2(a)(ii) A a B.

<sup>137</sup> Viz EO 14086, § 2(c)(iv)B

<sup>138</sup> Viz EO 14086, § 2(b)(i)A, body 1 až 12.

<sup>139</sup> Viz EO 14086, § 2(c)(ii)A.

<sup>140</sup> Viz EO 14086, § 2(b)(ii)A, body 1 až 5.

<sup>141</sup> Viz EO 14086, § 2(b)(i)B.

<sup>142</sup> Rozsudek SDEU ve věci Schrems I, bod 92.

<sup>143</sup> Viz rozsudek SDEU ve věci Schrems II.



jak bylo připomenuto výše, že možnost hromadného shromažďování, „v důsledku které lze v rámci sledovacích programů, jejichž základem je EO 12333, přistupovat k údajům na cestě do Spojených států, přičemž takový přístup nepodléhá vůbec žádnému soudnímu dohledu, přitom rozhodně neohraničuje dostatečně jasně a přesně rozsah takového hromadného shromažďování osobních údajů“.

134. EDPB proto konstatuje, že SDEU hromadné shromažďování v zásadě nevyločil, ale ve svém rozhodnutí ve věci Schrems II dospěl k závěru, že aby takové hromadné shromažďování probíhalo zákonně, musí existovat dostatečně jasné a přesné limity, které ohraničí rozsah takového hromadného shromažďování.
135. EDPB rovněž bere na vědomí, že dekret EO 14086 nahrazuje směrnici PPD-28 a zároveň poskytuje nové záruky a omezení pro shromažďování a používání údajů shromážděných mimo USA, neboť se nepoužijí omezení stanovená zákonem FISA nebo jinými konkrétnějšími právními předpisy USA.
136. Pokud jde o hromadné shromažďování údajů, EDPB bere na vědomí, že dekret EO 14086 stanoví, že hromadné shromažďování je i nadále povoleno. EDPB zdůrazňuje, že definice hromadného shromažďování zůstává stejná jako v předchozí směrnici PPD-28: „*informacemi shromažďovanými hromadně prostřednictvím signálového zpravodajství se rozumí povolené shromažďování velkého množství údajů signálového zpravodajství, které jsou z technických nebo provozních důvodů získávány bez použití diskriminantů (například bez použití specifických identifikátorů nebo selekčních termínů)*“<sup>144</sup>.
137. Od rozhodnutí ve věci Schrems II Soudní dvůr přesně nedefinoval záruky vyžadované pro hromadné shromažďování. EDPB však připomíná, že EÚLP vydal důležitá rozhodnutí týkající se hromadného shromažďování a příslušných záruk v této souvislosti.
138. EDPB připomíná, že vzhledem k tomu, že hromadné shromažďování umožňuje shromažďování velkého množství údajů bez diskriminantů, představuje vyšší riziko pro fyzické osoby<sup>145</sup> než cílené shromažďování, a proto vyžaduje zavedení dodatečných záruk.
139. EDPB rovněž konstatuje, že SDEU vypracoval další judikaturu týkající se uchovávání údajů o provozu a lokačních údajů a následného přístupu k těmto údajům uchovávaným provozovateli telekomunikací, a to i pro účely národní bezpečnosti, které sice nelze v této souvislosti považovat za přímo použitelné, ale mohly by být do určité míry relevantní v souvislosti se stávajícím posouzením hromadného shromažďování v kontextu dekretu EO 12333.

#### 1) Omezení účelu

140. Dekret EO stanoví, že hromadné shromažďování by mělo být prováděno pouze na základě zjištění, že „*informace nezbytné k prosazení uznané zpravodajské priority nelze přiměřeně získat cíleným shromažďováním*“<sup>146</sup> a že „*daný prvek zpravodajské služby použije přiměřené metody a technická opatření s cílem omezit shromažďované údaje pouze na to, co je nezbytné k prosazení uznané zpravodajské priority při současné minimalizaci shromažďování irelevantních informací*“<sup>147</sup>. Kromě

---

<sup>144</sup> Viz EO 14086, § 4(b).

<sup>145</sup> Viz například ESLP (Velký senát) ve věci Big Brother Watch a ostatní v. Spojené království ze dne 25. května 2021 (dále jen „rozsudek ESLP ve věci Big Brother Watch“), bod 363, kde soud uvádí, že „*není přesvědčen o tom, že získávání souvisejících komunikačních dat prostřednictvím hromadného zachycování je nutně méně rušivé než získávání obsahu*“.

<sup>146</sup> EO 14086, § 2(c)(ii)(A).

<sup>147</sup> EO 14086, § 2(c)(ii)(A).

těchto záruk EDPB rovněž uznává, že se hromadně shromážděné údaje použijí ke splnění jednoho nebo více z uvedených šesti cílů<sup>148</sup>. EDPB dále zdůrazňuje, že ačkoli jsou tyto cíle podrobnější než ty, které byly uvedeny v předchozí směrnici PPD-28, která byla obecně nahrazena dekretem EO 14086, rozsah takových možností shromažďování zůstává potenciálně i nadále široký, tj. zahrnuje velké objemy údajů.

141. EDPB zde rovněž připomíná, že dekret EO 14086 stanoví také možnost, aby prezident USA doplnil na seznam další cíle (viz bod 115)<sup>149</sup>.

### 2) Předchozí nezávislé povolení

142. EDPB zdůrazňuje, že ESLP přikládá značný význam předchozímu nezávislému povolení v souvislosti s hromadným shromažďováním údajů pro účely národní bezpečnosti. Soud totiž zejména rozhodl, že *„aby bylo minimalizováno riziko zneužití hromadného sledování, má soud za to, že celý proces musí podléhat zárukám od počátku až do konce, což znamená, že na vnitrostátní úrovni musí být v každé fázi tohoto procesu provedeno zhodnocení nezbytnosti a přiměřenosti přijímaných opatření; že hromadné zachycování musí podléhat nezávislému povolení již na samém počátku, kdy je vymezen cíl a rozsah operace; a že na průběh operace by mělo být dohlíženo a musí podléhat následnému nezávislému přezkumu. Podle názoru soudu se jedná o základní záruky, které budou základním kamenem každého režimu hromadného zachycování, který je v souladu s článkem 8.“*<sup>150</sup>
143. EDPB rovněž poukazuje na následující odstavec tohoto rozsudku velkého senátu, v němž štrasburský soud dále zdůrazňuje, že *„souhlasí se senátem v tom smyslu, že povolení soudu je sice „důležitou zárukou proti svévoli“, ale není „nezbytným požadavkem“ (viz body 318–320 rozsudku senátu). Hromadné zachycování by však mělo být schváleno nezávislým orgánem; tj. orgánem, který je nezávislý na výkonné moci“*<sup>151</sup>.
144. EDPB v této souvislosti konstatuje, že dotčený dekret takové nezávislé předchozí povolení pro hromadné shromažďování údajů nevyžaduje, a že není uvedeno ani v dekretu EO 12333 (viz oddíl níže týkající se dekretu EO 12333).

### 3) Pravidla uchovávání

145. EDPB připomíná, že dalším důležitým souborem záruk jsou pravidla upravující dobu shromažďování a uchovávání údajů. ESLP v tomto ohledu zdůraznil, že *„vnitrostátní právo by mělo zakotvovat omezení délky zachycování, postup, který je třeba dodržet při zkoumání, použití a uchovávání získaných údajů, opatření, která mají být přijata při sdělování údajů jiným stranám, a okolnosti, za nichž musí být zachycené údaje vymazány nebo zničeny“*<sup>152</sup>, protože tyto záruky *„jsou pro hromadné zachycování relevantní ve stejné míře“*<sup>153</sup>.
146. V tomto ohledu má EDPB za to, že dekret EO stanoví pravidla týkající se uchovávání údajů pro osobní údaje shromážděné prostřednictvím signálového zpravodajství, a to i na základě hromadného shromažďování<sup>154</sup>. EDPB konstatuje, že podle § 2 písm. c) bodu iii) podbodu A dekretu EO 14086 každý prvek zpravodajské služby, který nakládá s osobními informacemi shromážděnými prostřednictvím signálového zpravodajství, stanoví a uplatňuje politiky a postupy určené k minimalizaci šíření a

<sup>148</sup> EO 14086, § 2(c)(ii)(B).

<sup>149</sup> Viz EO 14086, § 2(c)(ii)(C).

<sup>150</sup> Viz rozsudek ESLP ve věci Big Brother Watch, bod 350.

<sup>151</sup> Viz rozsudek ESLP ve věci Big Brother Watch, bod 351.

<sup>152</sup> Viz rozsudek ESLP ve věci Big Brother Watch, bod 348.

<sup>153</sup> Viz rozsudek ESLP ve věci Big Brother Watch, bod 348.

<sup>154</sup> Viz EO 14086, § 2(c)(iii)(A)(2)(a)–(c).

uchovávání osobních informací shromážděných prostřednictvím signálového zpravodajství. Tato pravidla však nestanoví konkrétní dobu uchovávání, ale spíše obecně odkazují na stejná platná pravidla pro uchovávání údajů týkajících se občanů USA a na situace, kdy nebylo provedeno konečné rozhodnutí o uchovávání. EDPB je proto znepokojen tím, že tyto doby uchovávání, pokud jde o cílené shromažďování (viz bod 122), nejsou v tomto dekretu EO jasně definovány, pokud jde o hromadně shromažďované údaje. Vyzývá Komisi, aby sdílela své posouzení nezbytnosti a přiměřenosti dob uchovávání platných pro občany USA a dostupné informace týkající se dob uchovávání v praxi v případě, že nebylo vydáno konečné rozhodnutí o uchovávání údajů podle právních předpisů USA, neboť návrh rozhodnutí ve své současné podobě připomíná toto obecné pravidlo pouze v jediném krátkém odstavci<sup>155</sup> a v poznámce pod čarou<sup>156</sup>, což neumožňuje určit, zda jsou tyto doby uchovávání nezbytné a přiměřené. Vzhledem k tomu, že, jak zdůraznil ESLP, se jedná o zásadní záruku umožňující subjektům údajů uplatňovat svá práva především v situaci, kdy je přijímáno obzvláště obtěžující opatření ke shromažďování jejich údajů, vyzývá EDPB Evropskou komisi, aby poskytla další vysvětlení týkající se různých dob uchovávání v praxi.

#### 4) Záruky týkající se „šíření“

147. EDPB rovněž připomíná, že pro zajištění účinnosti zásady nezbytnosti a přiměřenosti a zásady účelového omezení ESLP rovněž uznal význam pravidel stanovených právními předpisy, která se týkají dalšího šíření shromážděných údajů, a to i v souvislosti s hromadným shromažďováním<sup>157</sup>.
148. Ustanovení § 2(c)(iii)(A)(1)(c) dekretu EO 14086 stanoví, že informace o osobách, které nejsou občany USA, shromážděné prostřednictvím signálového zpravodajství, lze šířit pouze tehdy, nabude-li oprávněná a náležitě vyškolená fyzická osoba důvodného přesvědčení, že tyto osobní informace budou náležitě chráněny a že příjemce potřebuje tyto informace znát.
149. S ohledem na tuto skutečnost má EDPB za to, že ustanovení týkající se šíření informací podle dekretu EO 14086 nestanoví ani výslovný zákaz šíření informací pro jiné účely než pro účely národní bezpečnosti, pokud jde o jejich předávání příslušným orgánům USA<sup>158</sup>. EDPB vyzývá Komisi, aby v tomto případě podrobněji objasnila platná pravidla a záruky.
150. EDPB je proto znepokojen tím, že údaje získané příslušnými orgány zpravodajské služby by následně mohly být předány příslušným orgánům USA za účelem boje proti trestné činnosti včetně závažných trestných činů v rámci trestního vyšetřování, čímž by byla donucovacím orgánům bez jakýchkoli dalších zvláštních omezení poskytnuta možnost získat údaje, jejichž přímé shromažďování by jim bylo zakázáno, a vyzývá Komisi k dalšímu posouzení tohoto bodu.
151. Ve specifickém kontextu dalšího předávání (šíření ve vztahu k příjemcům mimo vládu USA včetně zahraničních vlád nebo mezinárodních organizací<sup>159</sup>) EDPB připomíná, že je toho názoru, že ochrana údajů by měla být zachována i v souvislosti s dalším předáváním, a to včetně oblasti národní bezpečnosti<sup>160</sup>.

---

<sup>155</sup> Viz návrh rozhodnutí, bod 150.

<sup>156</sup> Viz návrh rozhodnutí, poznámka pod čarou 271.

<sup>157</sup> Viz rozsudek ESLP ve věci Big Brother Watch, bod 348.

<sup>158</sup> Viz EO 14086, § 2(c)(iii)(A)(1).

<sup>159</sup> Viz EO 14086, § 2(c)(iii)(A)(1), zejména písm. d).

<sup>160</sup> Viz například stanovisko EDPB 14/2021 k návrhu prováděcího rozhodnutí Evropské komise podle nařízení (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů ve Spojeném království. Přijato dne 13. dubna 2021, oddíly 4.3.2.1 a 4.3.2.2.

152. V tomto ohledu dekret EO stanoví určité záruky, konkrétně požadavek řádně zohlednit účel šíření – aniž by však výslovně požadoval, aby účelem šíření byla rovněž ochrana národní bezpečnosti – povahu a rozsah šířených osobních informací a potenciální škodlivý dopad na dotčenou osobu nebo osoby před šířením údajů.
153. Přestože EDPB uznává, že některé z těchto záruk, zejména skutečnost, že je třeba zohlednit „*potenciální škodlivý dopad*“<sup>161</sup> na dotčený subjekt (dotčené subjekty) údajů, odrážejí některé požadavky EÚLP, zdůrazňuje také, že štrasburský soud dále vyžaduje právně závaznou povinnost „*zkoumat a ověřit, zda zahraniční příjemce zpravodajských informací poskytne akceptovatelnou minimální úroveň záruk*“<sup>162</sup>, kterou EDPB nenachází výslovně uvedenou v ustanoveních dekretu týkajících se zpřístupnění informací zahraničním příjemcům. EDPB proto vyzývá Komisi, aby tento prvek dále posoudila.
154. EDPB rovněž konstatuje, že Evropská komise v rámci svého hodnocení odpovídající úrovně ochrany nevezala v úvahu existenci mezinárodních dohod uzavřených se třetími zeměmi nebo mezinárodními organizacemi, které mohou stanovit zvláštní ustanovení pro mezinárodní předávání osobních údajů zpravodajskými službami do třetích zemí. EDPB má za to, že uzavírání dvoustranných nebo mnohostranných dohod se třetími zeměmi pro účely zpravodajské spolupráce pravděpodobně ovlivní posuzovaný právní rámec pro ochranu údajů.
155. EDPB proto vyzývá Evropskou komisi, aby objasnila, zda takové dohody existují a za jakých podmínek mohou být uzavírány, a aby posoudila, zda ustanovení mezinárodních dohod mohou ovlivnit úroveň ochrany osobních údajů předávaných z EHP poskytovanou legislativním rámcem a postupy týkající se dalšího předávání pro účely národní bezpečnosti.

5) *Dočasné hromadné shromažďování na podporu počáteční technické fáze cíleného shromažďování*

156. EDPB připomíná, že diskuse v souvislosti s posledním společným přezkumem štítu na ochranu soukromí se zaměřovaly především na výklad a uplatňování dodatečného důvodu (situace/scenáře) pro hromadné shromažďování podle první věty poznámky pod čarou 5 v § 2 směrnice PPD-28, podle níž se „*omezení obsažená v tomto paragrafu nevztahují na údaje signálového zpravodajství, které jsou dočasně získávány za účelem usnadnění cíleného shromažďování*“. Orgány USA zároveň vysvětlily význam pojmu „*údaje signálového zpravodajství, které jsou dočasně získávány za účelem usnadnění cíleného shromažďování*“. EDPB z těchto diskusí vyrozuměl, že uvedená poznámka pod čarou znamená, že údaje mohou být shromažďovány hromadně (a to bez ohledu na šest předpokládaných účelů), pokud jsou shromažďovány dočasně s cílem určit identifikátor pro stanovený cíl. Jednalo by se tedy o dodatečný důvod pro hromadné shromažďování údajů, a v tomto případě by nadále platily pouze obecné zásady § 1 směrnice PPD-28. Jak je uvedeno výše, v rozsudku ve věci Schrems II měl SDEU za to, že kombinace dekretu EO 12333 a směrnice PPD-28 ve vztahu k hromadnému shromažďování údajů „*neohraničuje dostatečně jasně a přesně rozsah takového hromadného shromažďování osobních údajů*“<sup>163</sup>.

<sup>161</sup> Viz EO 14086, § 2(c)(iii)(A)(1)(d).

<sup>162</sup> Viz rozsudek ESLP (velkého senátu) ve věci Centrum För Rättvisa v. Švédsko ze dne 25. května 2021, bod 326.

<sup>163</sup> Rozsudek SDEU ve věci Schrems II, bod 183.

157. EDPB konstatuje, že dekret EO 14086<sup>164</sup> i nadále stanoví výjimku umožňující tento druh hromadného shromažďování, nicméně vítá, že tato výjimka byla oproti směrnici PPD-28 zúžena a že v rámci dekretu EO 14086 jsou stanoveny další záruky.
158. EDPB si je vědom toho, že nový dekret EO 14086 stanoví záruky, které jsou i nadále použitelné v souvislosti s tímto typem dočasně technického hromadného shromažďování, zejména obecné zásady nezbytnosti a přiměřenosti ve vztahu k uznané zpravodajské prioritě v případech, kdy jsou údaje získávány bez využití diskriminantů dříve, než je provedeno cílené shromažďování (EO 14086, § 2(a)–(b), § 2(c)(i)). Evropský sbor rovněž vyrozuměl, že takovéto hromadné shromažďování podporující následné cílené shromažďování v rámci signálového zpravodajství rovněž podléhá dodatečným zárukám poskytovaným na základě § 2(c)(iii) a následujících ustanovení<sup>165</sup>.
159. EDPB však rovněž připomíná (viz bod 117 výše), že definice „uznané zpravodajské priority“ stanoví postup pro výjimku, která by nezahrnovala účast CLPO z Úřadu ředitele národních zpravodajských služeb.
160. EDPB však i nadále konstatuje, že záruky uvedené v pododdíle týkajícím se hromadného shromažďování se nevztahují na dočasné hromadné shromažďování používané na podporu počáteční technické fáze cíleného shromažďování prostřednictvím signálového zpravodajství, jak je uvedeno v § 2(c)(ii)(D) dekretu EO 14086, což znamená zejména to, že v této souvislosti mohou být hromadně shromažďované údaje použity pro jiné účely než ty, které jsou uvedeny v § 2(c)(ii). EDPB by uvítal, kdyby v návrhu rozhodnutí byly vyjasněny účely, pro které mohou být hromadně shromážděné údaje v této souvislosti použity, jakož i uplatňování omezení stanovených v § 2(c)(i) pro shromažďování prostřednictvím signálového zpravodajství obecně (konkrétně pouze pro legitimní cíle tam uvedené) v souvislosti s dočasným hromadným shromažďováním údajů v návrhu rozhodnutí.
161. EDPB na závěr rovněž zdůrazňuje, že tato výjimka pro dočasné hromadné shromažďování s ohledem na cílené shromažďování a zbývající záruky, které mají být uplatněny, zůstává nejasná, zejména pokud jde o to, které záruky dekretu EO 14086 by se vztahovaly na kterou fázi (hromadné shromažďování, další cílené shromažďování), a vyzývá Komisi, aby tyto prvky dále posoudila a aby posuzovala tyto aspekty rovněž v praxi v budoucích společných přezkumech.
162. Kromě toho platí, že ačkoli EDPB rovněž dále vyjadřuje politování nad tím, že i když byl pojem „dočasné“ v dekretu objasněn o něco podrobněji než ve směrnici PPD-28, podle názoru EDPB to stále znamená, že hromadné shromažďování může pokračovat do té doby, dokud nebude stanoven cíl. V této souvislosti EDPB připomíná, že je nezbytné mít k dispozici jasná a přesná pravidla, a zdůrazňuje zde také klíčovou záruku, kterou tato pravidla pro subjekty údajů představují.
163. Závěrem lze konstatovat, že EDPB je ve vztahu k zárukám použitelným na hromadné shromažďování i nadále znepokojen tím, že navzdory dodatečným zárukám, které stanoví dekret EO 14086, je stále poskytována možnost hromadného shromažďování údajů, tj. bez diskriminantů, aniž by byly stanoveny klíčové záruky, jako je například předchozí povolení ke shromažďování těchto údajů – a to včetně odchýlné situace dočasně technického hromadného shromažďování – rovněž s přihlédnutím k potřebě dalšího objasnění a obavám vyjádřeným ohledně přísné zásady účelového omezení následného přístupu k údajům, jasných a přísných pravidel uchování údajů a přísnějších záruk týkající se šíření hromadně shromážděných údajů, a to i v souvislosti s dalším předáváním.

---

<sup>164</sup> Viz EO 14086, § 2(c)(ii)(D) a návrh rozhodnutí, poznámka pod čarou 226.

<sup>165</sup> Další informace o těchto ustanoveních viz předchozí oddíly.

164. EDPB obecně zdůrazňuje, že výše uvedené rozhodnutí ESLP opět ukazuje význam komplexního dohledu ze strany nezávislých dozorových úřadů. EDPB zdůrazňuje, že nezávislý dohled ve všech fázích procesu přístupu vládních institucí pro účely národní bezpečnosti je důležitou zárukou proti svévolným sledovacím opatřením, a tudíž i pro posouzení odpovídající úrovně ochrany údajů. Záruka nezávislosti dozorových úřadů ve smyslu čl. 8 odst. 3 Listiny má za úkol zajistit účinné a spolehlivé monitorování dodržování pravidel pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů. To platí zejména za okolností, kdy je fyzické osobě vzhledem k povaze tajného sledování znemožněno žádat o přezkum nebo se přímo účastnit přezkumného řízení před provedením sledovacího opatření nebo v jeho průběhu.
165. EDPB připomíná, že posouzení přiměřenosti podle jeho názoru závisí na všech okolnostech daného případu, zejména na účinnosti následného dohledu a zákonných opravných prostředků, které stanoví právní rámec.

#### 3.2.2.4 Právní rámec upravující zvláštní shromažďování údajů pro účely národní bezpečnosti prováděné prvky zpravodajské služby na území USA i mimo ně

166. Ve svém rozhodnutí ve věci Schrems II SDEU v souvislosti s § 702 zákona FISA zdůraznil, že z tohoto textu „*nijak nevyplývá, že by existovala sebemenší omezení pro jím stanovené zmocnění k provádění sledovacích programů za účelem získání zahraničních zpravodajských informací nebo že by existovaly záruky pro osoby, které nejsou osobami USA a na které se tyto programy mohou vztahovat*“<sup>166</sup>. To vedlo Soudní dvůr k závěru, že „*za těchto podmínek (...), nemůže tento článek zajistit takovou úroveň ochrany, která by byla v zásadě rovnocenná úrovni ochrany zaručené Listinou, (...) podle které právní základ dovolující zásahy do základních práv musí k tomu, aby byl v souladu se zásadou proporcionality, sám definovat rozsah omezení výkonu dotyčného práva a také stanovit jasná a přesná pravidla pro rozsah a použití předmětného opatření a stanovit minimální požadavky*“<sup>167</sup>.
167. Ve vztahu k dekretu EO 12333 Soudní dvůr konstatoval, že „*nepřiznává práva vymahatelná vůči orgánům USA před soudy*“<sup>168</sup>, a rovněž dospěl k závěru, že „*lze v rámci sledovacích programů, jejichž základem je EO 12333, přistupovat k údajům na cestě do Spojených států, přičemž takový přístup nepodléhá vůbec žádnému soudnímu dohledu, přitom rozhodně neohraničuje dostatečně jasně a přesně rozsah takového hromadného shromažďování osobních údajů*“<sup>169</sup> v návaznosti na analýzu podmínek, za nichž by mohlo být prováděno hromadné shromažďování podle tohoto dekretu ve spojení s PPD-28.
168. Pokud jde o tyto zvláštní režimy shromažďování údajů, dekret EO 14086 nyní stanoví nová pravidla.

#### 3.2.2.4.1 Shromažďování údajů pro účely národní bezpečnosti podle § 702

169. EDPB připomíná, že v poslední zprávě výboru PCLOB uvítal zjištění týkající se § 702 zákona FISA<sup>170</sup>, podle nichž „*v praxi jsou omezení přístupu a uchování údajů, která jsou nezbytná pro účely minimalizačních postupů a/nebo postupů pro zacílení jednotlivých agentur, uplatňována i na osoby, které nejsou občany USA, a to z důvodu nákladnosti a obtížnosti identifikace občanů USA a odstranění informací o nich u velkého souboru údajů, což znamená, že obvykle je s celým souborem údajů nakládáno v souladu s vyššími standardy pro údaje platnými pro USA.*“

<sup>166</sup> Viz rozsudek SDEU ve věci Schrems II, bod 180.

<sup>167</sup> Viz rozsudek SDEU ve věci Schrems II, bod 180.

<sup>168</sup> Viz rozsudek SDEU ve věci Schrems II, bod 182.

<sup>169</sup> Viz rozsudek SDEU ve věci Schrems II, bod 183.

<sup>170</sup> Viz zpráva výboru PCLOB o programu sledování prováděném podle § 702 FISA, strana 100.

170. Podle těchto zjištění „*tento program nefunguje na základě hromadného shromažďování komunikace*“. Toto zjištění potvrdily i zprávy Statistical Transparency Reports z let 2014 a 2021 vydané Úřadem ředitele národních zpravodajských služeb. Podle zprávy výboru PCLOB jsou navíc pro zacílení dohledu používány „zadané selektory“, jako je například e-mailová adresa nebo telefonní číslo.
171. EDPB však rovněž připomíná, že v souvislosti s § 702 bylo při posledním přezkumu štítu na ochranu soukromí zároveň vyjasněno, že „osobou“, která má být identifikována jako cíl, se může rozumět více fyzických osob používajících stejný identifikátor za předpokladu, že všechny tyto fyzické osoby jsou osobami, které nejsou občany USA, a že splňují příslušná kritéria pro zacílení. EDPB rovněž připomíná, že během třetího každoročního společného přezkumu štítu na ochranu soukromí v roce 2019 bylo požadováno další vyjasnění v souvislosti s programem UPSTREAM s cílem vyloučit tento masivní a nahodilý přístup k osobním údajům osob, které nejsou občany USA<sup>171</sup>.
172. EDPB navíc připomíná, že skutečnost, že shromažďování informací podle § 702 FISA je odůvodněno tím, že „*důležitým účelem získávání informací je získání zahraničních zpravodajských informací*“, stále ponechává určitou nejistotu ohledně jeho účelového omezení a nezbytnosti. EDPB však konstatuje, že podle § 2 písm. a) bodů A a B dekretu EO 14086 lze činnosti signálového zpravodajství provádět pouze na základě zjištění, že tyto činnosti jsou nezbytné k prosazení uznané priority, a to pouze v rozsahu a způsobem, který je ve vztahu k této prioritě přiměřený, a že musí být v nejvyšší možné míře uzpůsobeny prosazení této uznané priority, přičemž se řádně zohlední příslušné faktory, jako je míra narušování soukromí v důsledku shromažďování informací a citlivost údajů, a zároveň nesmí být nepřiměřeně ovlivněno soukromí a občanské svobody. EDPB přesto očekává další objasnění toho, jak to bude konkrétně zaváděno a realizováno, a to i v souvislosti s uplatňováním § 702 zákona FISA.
173. V tomto ohledu EDPB vzhledem k tomu, že sám nemá přímý přístup k těmto informacím, vyzval k nezávislému posouzení nezbytnosti a přiměřenosti definice „cílů“ a pojmu „zahraniční zpravodajské informace“ podle § 702 FISA (a to i v kontextu programu UPSTREAM) po jeho obnovení. EDPB má za to, že jeho předchozí výzva k dalšímu nezávislému posouzení procesu uplatňování selektorů v konkrétních případech („úkolování selektorů“), jakož i k dalšímu objasnění v souvislosti s programem UPSTREAM je relevantní. EDPB proto při zohlednění nového dekretu EO 14086 vyzývá k poskytnutí dalších informací, aby bylo možné posoudit a sledovat rovněž to, jak a do jaké míry budou v této souvislosti v praxi uplatňovány nově zavedené zásady nezbytnosti a přiměřenosti, a očekává, že to bude posuzováno i v rámci budoucích společných přezkumů.
174. EDPB vítá, že plně funkční Výbor pro dohled nad ochranou soukromí a občanských svobod (PCLOB) se jako nezávislá agentura dohledu rozhodl provést „projekt v oblasti dohledu s cílem přezkoumat program sledování, který provozuje výkonná moc podle § 702 zákona o dohledu nad zahraniční informační službou (FISA) v očekávání data ukončení platnosti § 702 v prosinci 2023 a nadcházejícího projednávání jeho opětovného schválení veřejností a Kongresem“<sup>172</sup>. EDPB rovněž vítá, že tento „přezkum zahrnuje vybrané oblasti, na které se zaměřuje vyšetřování, včetně mimo jiné dotazů občanů USA na informace shromážděné podle § 702 a informace shromážděné v rámci programu „Upstream“ podle § 702“<sup>173</sup>, a „zahrnuje rovněž přezkum minulé a předpokládané hodnoty a účinnosti tohoto programu, jakož i přiměřenosti stávajících záruk ochrany soukromí a občanských svobod“<sup>174</sup>. EDPB v důsledku toho zdůrazňuje nezbytnost přístupu ke zjištěním výboru PCLOB v této zprávě o § 702

---

<sup>171</sup> Viz třetí zpráva o společném přezkumu, strana 17, bod 83.

<sup>172</sup> Viz [oznámení výboru PCLOB o projektu dohledu, který přezkoumává § 702 zákona o dohledu nad zahraniční informační službou \(FISA\)](#).

<sup>173</sup> Viz výše.

<sup>174</sup> Viz výše.

z hlediska přiměřeného a komplexního posouzení záruk ochrany soukromí poskytovaných a uplatňovaných v souvislosti s tímto programem sledování.

175. EDPB po zohlednění nového dekretu EO 14086 rovněž požaduje další informace, aby byl schopen posoudit a sledovat také to, jak a do jaké míry budou v této souvislosti v praxi uplatňovány nově zavedené zásady nezbytnosti a přiměřenosti, jakož i další záruky stanovené v tomto textu.

#### *3.2.2.4.2 Shromažďování údajů pro účely národní bezpečnosti podle dekretu EO 12333*

176. Jak uznal SDEU v rozsudku Schrems II, analýza právních předpisů třetí země, u níž se posuzuje odpovídající ochrana, by se neměla omezovat pouze na právní předpisy a postupy umožňující dohled v rámci fyzických hranic této země, ale měla by zahrnovat také analýzu právních důvodů v uvedených právních předpisech této třetí země, které jí umožňují provádět dohled mimo její území ve vztahu k údajům EU. Nezbytná omezení vládního přístupu k údajům by se měla vztahovat i na osobní údaje „na cestě“ do země, u níž je uznána odpovídající ochrana.
177. EDPB vítá zprávu pro potřeby široké veřejnosti, kterou vydal výbor PCLOB ohledně dekretu EO 12333 a která byla zveřejněna v dubnu 2021, ale konstatuje, že tato zpráva má i nadále obecný charakter, neboť většina zjištění je utajovaná.
178. V této souvislosti EDPB znovu zdůrazňuje význam očekávaných zpráv výboru PCLOB ohledně tohoto textu<sup>175</sup> vzhledem k nejistotě a nejasnostem ohledně toho, jak byl dekret EO 12333 uplatňován dříve, a vzhledem k důležitosti vyjasnění toho, jak bude uplatňován v budoucnu s ohledem na nový dekret EO 14086. Je si však vědom toho, že většina jejich obsahu pravděpodobně zůstane i nadále utajena, takže veřejnosti ani EPDB nebudou poskytnuty žádné další informace o konkrétním fungování dekretu EO 12333 ani o jeho nezbytnosti a přiměřenosti.
179. EDPB by proto uvítal zejména to, aby zpráva výboru PCLOB o uplatňování dekretu EO 14086 nebyla utajena, ale aby byla po svém dokončení zpřístupněna v plném rozsahu, a to včetně částí obsahujících posouzení toho, jak budou uplatňovány záruky dekretu EO 14086 na shromažďování údajů podle dekretu EO 12333. EDPB rovněž vyzývá Komisi, aby tomuto bodu věnovala obzvláštní pozornost v souvislosti s budoucími společnými přezkumy.
180. Obecně platí, že pokud jde o jednotlivé právní nástroje, které v právním rámci USA umožňují zpravodajským agenturám shromažďovat údaje a dále k nim přistupovat a zpracovávat je, EDPB by uvítal objasnění jejich vzájemného působení s novým dekretem EO 14086 a očekává ujištění, že dřívější obavy vyjádřené v předchozích stanoviscích EDPB v tomto ohledu budou přijetím těchto nových záruk vyřešeny.
181. EDPB rovněž vyzývá Komisi, aby těmto aspektům věnovala obzvláštní pozornost v souvislosti s budoucími společnými přezkumy.

---

<sup>175</sup> Obecná zpráva o dekretu EO 12333 zůstala z větší části utajena – zveřejněna byla pouze její krátká verze určená veřejnosti, a stejně tomu bylo i v případě zprávy a doporučení týkající se protiteroristických aktivit CIA prováděných na základě dekretu EO 12333 (Recommendations on CIA Counterterrorism Activities Conducted Pursuant to E.O.12333), která byla rovněž odtažena pouze částečně.



### 3.2.2.4.3 Zpráva výboru PCLOB

182. EDPB vítá, že dekret EO 14086 rovněž stanoví požadavek, aby výbor PCLOB vypracoval zprávu o provádění dekretu. EDPB zdůrazňuje, že tato zpráva by měla zahrnovat posouzení této konkrétní možnosti shromažďování údajů, kterou tento dekret poskytuje, pro účely uvedené jak pro cílené, tak i hromadné shromažďování, a to i z technických důvodů, aby bylo možné lépe porozumět klíčovým pojmům dekretu EO 14086 a tomu, jak jsou prakticky chápány a uplatňovány v jednotlivých programech sledování. Tato zpráva by byla rovněž nezbytná k posouzení toho, jak bude daný dekret prováděn ve vnitřních postupech a politikách prvků zpravodajských služeb.

### 3.2.3 Záruka C – Dohled

#### 3.2.3.1 Úvod

183. Zpravodajské činnosti USA podléhají procesu víceúrovňového dohledu. Strukturu dohledu v USA lze rozdělit na interní a externí dohled. Všechny prvky zpravodajských služeb mají úředníky pro dohled a soulad, kteří provádějí pravidelný dohled nad činnostmi signálového zpravodajství, včetně úředníků pro ochranu údajů a občanských svobod a generálních inspektorů. Kromě toho existují orgány externího dohledu, jako je například Výbor pro dohled nad ochranou soukromí a občanských svobod (PCLOB) a Výbor pro dohled nad zpravodajstvím.
184. EDPB připomíná, že k zásahu dochází v okamžiku shromažďování údajů, ale také v okamžiku, kdy k údajům získá přístup orgán veřejné moci za účelem jejich dalšího zpracování. ESLP několikrát upřesnil, že jakýkoli zásah do práva na soukromí a ochranu údajů by měl podléhat účinnému, nezávislému a nestrannému systému dohledu, který musí zajišťovat buď soudce, nebo jiný nezávislý subjekt<sup>176</sup> (např. správní orgán nebo parlamentní orgán).
185. ESLP se sice vyjádřil, že dává přednost tomu, aby za výkon dohledu odpovídal soudce, nevyločil však, že odpovědnost může nést i jiný subjekt, „*jestliže je dostatečně nezávislý na výkonné moci*“<sup>177</sup> a „*na orgánech provádějících sledování a jsou mu svěřeny dostatečné pravomoci a kompetence vykonávat účinnou a trvalou kontrolu*“<sup>178</sup>.
186. ESLP doplnil, že při posuzování nezávislosti je třeba zohlednit „*způsob jmenování a právní postavení členů orgánu dozoru*“<sup>179</sup>.
187. ESLP rovněž uvedl, že je třeba přezkoumat, zda činnosti orgánu dozoru podléhají veřejné kontrole. Toho by bylo možné dosáhnout například každoročním předkládáním zpráv o dohledu vládě, resp. pokud by veřejné zprávy byly předkládány parlamentu a parlament je projednával<sup>180</sup>.
188. Nezávislý dohled nad prováděním sledovacích opatření zohlednil také SDEU v rozsudku ve věci Schrems II, neboť „*[...] cílem přezkumu prováděného Soudem pro uplatňování zákona FISA je ověřit, zda tyto*

---

<sup>176</sup> Rozsudek ESLP ve věci Klass a další v. Německo ze dne 6. září 1978 (dále jen „rozsudek ESLP ve věci Klass“), body 17 a 51.

<sup>177</sup> Rozsudek ESLP ve věci Zakharov, bod 258; rozsudek ESLP ve věci Lordachi a další v. Moldavsko ze dne 10. února 2009, body 40 a 51; rozsudek ESLP ve věci Dumitru Popescu v. Rumunsko ze dne 26. dubna 2007, body 70–73.

<sup>178</sup> Rozsudek ESLP ve věci Klass, bod 56.

<sup>179</sup> Rozsudek ESLP ve věci Zakharov, bod 278.

<sup>180</sup> Rozsudek ESLP ve věci Zakharov, bod 283; rozsudek ESLP ve věci L. v. Norsko ze dne 9. června 1990; rozsudek ESLP ve věci Kennedy v. Spojené království ze dne 18. května 2010, bod 166.

*sledovací programy odpovídají cíli získat zahraniční zpravodajské informace, ale nikoli, zda jsou za účelem získání zahraničních zpravodajských informací fyzické osoby cíleny správně“<sup>181</sup>.*

### 3.2.3.2 Interní dohled

#### 3.2.3.2.1 Generální inspektoři

189. Evropský sbor pro ochranu údajů konstatuje, že generálním inspektorům je svěřena široká škála oprávnění, která jsou nezbytná ke sledování zpravodajských činností. Generální inspektoři mají zejména přístup ke všem informacím nezbytným k posouzení celkového souladu práce agentur s právními předpisy, mimo jiné včetně zákonů týkajících se soukromí a ochrany údajů, a mohou vydávat předvolání a přijímat přísahu od jakékoli osoby v souvislosti s vyšetřováním generálních inspektorů.
190. Na základě výše uvedených skutečností má EDPB za to, že generální inspektoři mají obecně rozsáhlé vyšetřovací pravomoci. Nemají však žádné závazné pravomoci umožňující zjednat nápravu a vydávají pouze nezávazná doporučení<sup>182</sup>.
191. EDPB konstatuje, že generálním inspektorům nesmí být v zásadě bráněno ani zakázáno zahájit, provádět nebo dokončit jakýkoli audit nebo vyšetřování nebo vydat předvolání v průběhu jakéhokoli auditu nebo vyšetřování<sup>183</sup>. V této souvislosti však EDPB konstatuje, že generální inspektoři spadají pod pravomoc, vedení a kontrolu příslušného vedoucího oddělení, který jim může zakázat přístup k informacím, provádění vyšetřování a mimo jiné i vydávání předvolání v případech, kdy vedoucí oddělení rozhodne, že takový zákaz je nezbytný pro ochranu národních zájmů. Vedoucí oddělení však musí o výkonu této pravomoci informovat odpovědné výbory Kongresu USA<sup>184</sup>.
192. EDPB konstatuje, že generální inspektory může odvolat pouze prezident USA, který musí Kongresu sdělit důvody pro takové odvolání.
193. EDPB konstatuje, že od vydání stanovisek pracovní skupiny zřízené podle článku 29 a poté sboru EDPB nedošlo k významným změnám mechanismu interního dohledu. EDPB z toho proto v souladu se stanoviskem pracovní skupiny zřízené podle článku 29 č. 1/2016<sup>185</sup> vyvozuje, že obecně jsou zavedeny dostatečné mechanismy interního dohledu.

#### 3.2.3.3 Externí dohled

194. EDPB konstatuje, že kromě níže uvedených orgánů dohlíží na činnost zpravodajských agentur USA i různé další orgány v rámci vlády USA, jako je například Výbor pro dohled nad zpravodajstvím (Intelligence Oversight Board, IOB) nebo výbory Kongresu. Tyto výbory mohou provádět vlastní vyšetřování a vypracovávat zprávy.

---

<sup>181</sup> Rozsudek SDEU ve věci Schrems II, bod 179.

<sup>182</sup> Návrh rozhodnutí, 105. bod odůvodnění.

<sup>183</sup> Zákon o generálních inspektorech (Inspector General Act) z roku 1978, § 3(a).

<sup>184</sup> Viz např. zákon o generálních inspektorech z roku 1978, § 8 (ve vztahu k ministerstvu obrany); § 8E (ve vztahu k ministerstvu spravedlnosti), § 8G(d)(2)(A),(B) (ve vztahu k NSA); hlava 50 U.S.C. § 403q(b) (ve vztahu k CIA); zákon o povolení zpravodajské činnosti pro fiskální rok 2010 (Intelligence Authorization Act For Fiscal Year 2010), § 405(f) (ve vztahu ke zpravodajským službám).

<sup>185</sup> Stanovisko skupiny WP 29 č. 1/2016.

### 3.2.3.3.1 Výbor pro dohled nad ochranou soukromí a občanských svobod (PCLOB)

195. EDPB uznává komplexní úlohu výboru PCLOB v oblasti dohledu nad novým nápravným mechanismem a prováděním dekretu EO 14086.
196. Za prvé, jeho nové funkce zahrnují konzultace s ministrem spravedlnosti, pokud jde o jmenování soudců odvolacího soudu pro ochranu údajů (DPRC) a zvláštních advokátů. Za druhé, výbor PCLOB bude každoročně přezkoumávat proces nápravy, tj. zpracovávání způsobilých stížností prostřednictvím mechanismu nápravy. To zahrnuje i to, zda CLPO a soud DPRC zpracovávaly způsobilé stížnosti včas, zda získávají plný přístup k nezbytným informacím a fungují v souladu s dekretem EO 14086, jakož i to, zda zpravodajské služby dodržují rozhodnutí CLPO a DPRC.
197. Výbor PCLOB musí být konzultován i tehdy, pokud zpravodajské služby USA aktualizují své vnitřní politiky a postupy k provádění dekretu EO 14086. Výbor PCLOB navíc provede přezkum aktualizovaných politik a postupů a posoudí jejich soulad s dekretem EO 14086<sup>186</sup>. Zjištění výboru PCLOB sice nejsou v úzkém slova smyslu závazná, avšak vedoucí každého prvku zpravodajských služeb je povinen pečlivě zvážit a provést nebo jinak řešit všechna doporučení obsažená v jakémkoli takovém přezkumu v souladu s platnými právními předpisy<sup>187</sup>. EDPB vyzývá Komisi, aby v případě, že bude návrh rozhodnutí přijat, v budoucích přezkumech věnovala zvláštní pozornost tomu, zda a jak jsou prováděna doporučení výboru PCLOB na úrovni agentur.
198. EDPB připomíná, že vzhledem k tomu, že výbor PCLOB je nezávislý, je „vybízen“ k tomu, aby přezkoumal, zda jsou řádně zohledňovány záruky stanovené v dekrete EO 14086 a zda zpravodajské služby v plném rozsahu splnily požadavky procesu nápravy, avšak není to jeho povinností. EDPB však má za to, že výbor PCLOB ve svém dodatečném vysvětlení pro EDPB i vůči veřejnosti<sup>188</sup> uvedl, že převezme úlohu předpokládanou v dekrete EO 14086.
199. EDPB rovněž vítá, že výsledky zpráv výboru PCLOB mají být zveřejněny. Vzhledem k tomu, že jednotlivé orgány v rámci nápravného mechanismu a orgány zpravodajských služeb jsou v zásadě povinny provádět doporučení uvedená ve zprávách výboru PCLOB nebo se jimi jinak zabývat, EDPB konstatuje, že tato doporučení hrají důležitou úlohu záruk týkajících se soukromí.
200. EDPB konstatuje, že přístup výboru PCLOB k informacím je omezen v případě, že prezident USA povolí provádění „utajených akcí“<sup>189</sup> ministerstvům, agenturám nebo subjektům vlády USA<sup>190</sup>.
201. V návaznosti na svá předchozí stanoviska považuje EDPB výbor PCLOB jakožto nezávislý orgán, jehož doporučení významně přispívají k reformám v USA a jehož zprávy jsou obzvláště užitečným zdrojem pro pochopení fungování jednotlivých programů sledování, za základní prvek struktury dohledu.
202. EDPB však ve svém třetím každoročním společném přezkumu bývalého štítu EU-USA na ochranu soukromí vyjádřil politování nad tím, že výbor PCLOB poskytl sboru EDPB pouze tytéž informace jako veřejnosti. Dále uvedl, že je politováníhodné, že výbor PCLOB nevydal v návaznosti na svou první zprávu

<sup>186</sup> EO 14086, § 2(c)(iv) a § 2(c)(v).

<sup>187</sup> EO 14086, § 2(c)(v)(B).

<sup>188</sup> [https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf)

<sup>189</sup> Podle hlavy 50 U.S.C. § 3093 písm. e) bodu 1 se pojmem „utajená akce“ rozumí činnost nebo činnosti vlády USA, jejíž cílem je ovlivnit politické, ekonomické nebo vojenské podmínky v zahraničí, kde se předpokládá, že role vlády USA nebude zřejmá nebo veřejně uznána, což však nezahrnuje 1) činnosti, jejichž primárním účelem je získávání zpravodajských informací, tradiční kontrarozvědná činnost [...].

<sup>190</sup> Hlava 42 U.S.C. § 2000ee(g)(5); hlava 50 U.S.C. § 3093(a).

i další zprávy o směrnici PPD-28 s cílem poskytnout další informace ohledně způsobu uplatňování záruk směrnice PPD-28, jakož i obecnou aktualizovanou zprávu o § 702 zákona FISA.

203. EDPB proto vítá oznámení výboru PCLOB, že v blízké budoucnosti lze očekávat zveřejnění následné zprávy týkající se § 702 zákona FISA. EDPB je rovněž spokojen s tím, že výbor PCLOB informoval o svém závazku umožnit zveřejnění svých zpráv týkajících se dekretu EO 14086. EDPB však připomíná, že zveřejňování neutajovaných zpráv je upraveno právními předpisy USA, musí být koordinováno s agenturami zpravodajských služeb a výbor PCLOB o nich nemůže rozhodovat z vlastní vůle.
204. Pokud tedy bude návrh rozhodnutí přijat, EDPB připomíná, že při budoucích přezkumech rámce EU-USA pro ochranu údajů by odborníci EDPB s bezpečnostní prověrkou měli mít možnost podle potřeby přezkoumat další dokumenty a projednat další utajované prvky s cílem zajistit náležité posouzení informací uvedených ve zprávách při současném zohlednění příslušných zájmů národní bezpečnosti a platné ochrany soukromí.
205. EDPB vítá nezávislost výboru PCLOB a jeho dohled nad vnitrostátními zpravodajskými službami, které musí dodržovat doporučení výboru PCLOB nebo se jimi jinak zabývat, což bude uvedeno ve zprávě výboru PCLOB pro Kongres USA.
206. S ohledem na požadavky ESLP týkající se veřejné kontroly<sup>191</sup>, podle nichž musí být zprávy orgánu dozoru předloženy parlamentu a projednány parlamentem, považuje EDPB za dostatečné, aby výbor PCLOB předkládal své zprávy nejméně dvakrát ročně prezidentovi USA a zejména výborům Kongresu v rámci Senátu a Sněmovny reprezentantů<sup>192</sup>, které jsou parlamentními orgány USA.

#### 3.2.3.3.2 Soud FISA (*Foreign Intelligence Surveillance Court, FISC*)

207. FISC odpovídá za dohled nad shromažďováním osobních údajů podle § 702 zákona FISA<sup>193</sup> a proti jeho rozhodnutím se lze odvolat k Odvolacímu soudu FISA (FISCR).
208. Soud FISC dohlíží na proces certifikace týkající se shromažďování zahraničních zpravodajských informací podle § 702 zákona FISA a povoluje elektronické sledování, fyzické prohlídky a další vyšetřovací prostředky pro účely zahraničního zpravodajství<sup>194</sup>. Soud FISC také schvaluje postupy pro cílení, minimalizaci a dotazování týkající se certifikátů, které jsou pro zpravodajské služby USA právně závazné<sup>195</sup>. Pokud FISC zjistí, že požadavky splněny nebyly, může certifikaci zcela nebo zčásti zamítnout a požadovat změnu postupů.
209. Jsou-li zjištěna porušení postupů zacílení, může FISC nařídit příslušné zpravodajské službě, aby přijala nápravná opatření<sup>196</sup>. Tato nápravná opatření mohou zahrnovat individuální i strukturální opatření, tj. opatření sahající od ukončení získávání údajů a výmazu protiprávně získaných údajů až po změnu postupu shromažďování údajů, včetně pokynů a školení pracovníků.

---

<sup>191</sup> Rozsudek ESLP ve věci Zakharov, bod 283, rozsudek ESLP ve věci L. v. Norsko ze dne 9. června 1990; rozsudek ESLP ve věci Kennedy v. Spojené království ze dne 18. května 2010, bod 166.

<sup>192</sup> Hlava 42 U.S.C. § 2000ee(e).

<sup>193</sup> Hlava 50 U.S.C. § 1881(a).

<sup>194</sup> [www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court](http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court)

<sup>195</sup> Hlava 50 U.S.C. § 1881a(i).

<sup>196</sup> Hlava 50 U.S.C. § 1803 (h).

210. EDPB bere na vědomí, že dekret EO 14086 stanoví, že CLPO a DPRC mají povinnost o porušení informovat náměstka ministra spravedlnosti pro otázky národní bezpečnosti, který tato porušení oznámí soudu FISC<sup>197</sup>.
211. Jak uvedl SDEU ve svém rozhodnutí ve věci Schrems II, FISC nepovoluje jednotlivá sledovací opatření, nýbrž povoluje celé sledovací programy<sup>198</sup>. EDPB je proto i nadále znepokojen tím, že FISC nezajišťuje účinný soudní dohled nad zacílením na osoby, které nejsou občany USA, což nový dekret EO 14086 zjevně neřeší.
212. Pokud jde o předchozí nezávislé povolení<sup>199</sup> sledování podle § 702 zákona FISA, EDPB s politováním konstatuje, že jak vyrozuměl z návrhu rozhodnutí<sup>200</sup> a z vysvětlení poskytnutých vládou USA, nejeví se, že by byl FISC při certifikaci programů povolujících cílení na osoby, které nejsou občany USA, vázán dodatečnými zárukami stanovenými v dekretu EO 14086. Podle názoru EDPB by však měly být dodatečné záruky uvedené v tomto dekretu v této souvislosti i přesto zohledňovány. EDPB připomíná, že zprávy výboru PCLOB by byly obzvláště užitečné pro posouzení toho, jak budou prováděny záruky uvedené v dekretu EO 14086 a jak jsou tyto záruky uplatňovány při shromažďování údajů podle § 702 zákona FISA.

### 3.2.4 Záruka D – Fyzické osoby musí mít k dispozici účinné opravné prostředky

213. EDPB připomíná, že účinná a vymahatelná práva fyzických osob mají zásadní význam pro zjištění odpovídající úrovně ochrany údajů ve třetí zemi. Subjekty údajů musí mít k dispozici účinný prostředek nápravy, aby prosadily svá práva, pokud se domnívají, že nejsou nebo nebyla dodržována. SDEU ve svých rozsudcích ve věcech Schrems I a II objasnil, že „právní úprava, která nestanoví procesním subjektům žádnou možnost využít právních prostředků s cílem získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu těchto údajů, nerespektuje podstatu základního práva na účinnou právní ochranu zakotveného v článku 47 Listiny“<sup>201</sup>.
214. Systém USA týkající se soudní ochrany obsahuje významné omezení, které velmi ztěžuje zahájení soudního řízení proti sledovacím opatřením vlády USA u běžných soudů. Ústava USA vyžaduje, aby fyzické osoby prokázaly legitimaci, tj. „konkrétní, specifikovanou a skutečnou nebo bezprostředně hrozící újmu“<sup>202</sup>. Zdá se, že v případech sledování se takový požadavek ruší v důsledku toho, že fyzické osoby podrobené sledování o tom nejsou informovány ani po ukončení těchto opatření.
215. V této souvislosti EDPB vítá, že dekret EO 14086 zavádí zvláštní nápravný mechanismus pro vyřizování a řešení stížností osob, které nejsou občany USA, ve vztahu k činnostem signálového zpravodajství USA. V rámci tohoto nového mechanismu výše uvedený požadavek na legitimaci uplatnit nelze: podle § 4 písm. k) bodu ii) dekretu EO 14086 nemusí žalobce prokazovat, že jeho údaje byly skutečně předmětem signálového zpravodajství USA. Subjekty údajů se tak mohou dovolávat záruk stanovených dekretem EO 14086 včetně záruk stanovených jinými příslušnými zákony a ustanoveními, jak je uvedeno v § 4

---

<sup>197</sup> EO 14086, § 3(c)(i)(D); EO 14086 § 3(d)(i)(F).

<sup>198</sup> Rozsudek SDEU ve věci Schrems II, bod 179.

<sup>199</sup> Pokud jde o hromadné shromažďování údajů podle dekretu EO 12333, které nespádá do příslušnosti FISC, EDPB je znepokojen tím, že není zaveden proces předchozího schvalování hromadného shromažďování údajů (viz rovněž záruka B).

<sup>200</sup> Návrh rozhodnutí, 165. bod odůvodnění.

<sup>201</sup> Rozsudek SDEU ve věci Schrems I, bod 95; rozsudek SDEU ve věci Schrems II, bod 187.

<sup>202</sup> Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II., s. 10.

písm. d) bodě iii) dekretu EO 14086<sup>203</sup>. Tento nový mechanismus tedy v tomto ohledu stanoví novou možnost nápravy, která by jinak neexistovala.

216. Nový mechanismus se skládá ze dvou vrstev: v rámci první vrstvy mohou fyzické osoby podávat stížnost u úředníka pro ochranu občanských svobod z Úřadu ředitele národních zpravodajských služeb (CLPO). Na druhé úrovni mají fyzické osoby možnost odvolat se proti rozhodnutí CLPO u nově vytvořeného orgánu, tzv. odvolacího soudu pro ochranu údajů (DPRC). Následující oddíly se zaměřují především na druhou úroveň tohoto mechanismu nápravy. EDPB má za to, že CLPO jakožto pověřený vládní úředník nemá dostatečnou míru nezávislosti na výkonné moci, a proto nemůže sám o sobě odpovídajícím způsobem plnit požadavky vyplývající z článku 47 Listiny. Komise toto posouzení několikrát potvrdila.

#### *3.2.4.1 Může být zřízení odvolacího soudu pro ochranu údajů (DPRC) na základě prezidentského dekretu samo o sobě dostačující?*

217. DPRC není běžným soudem zřízeným Kongresem podle článku III Ústavy USA, ale je založen na dekretu vydaném prezidentem USA. EDPB si je sice vědom úvahy, z níž tato skutečnost vychází, konkrétně vyhýbání se požadavku na legitimaci, a obecně ji vítá (viz také bod 215), avšak vyvstává zde zásadní otázka: může takový mechanismus nápravy (vůbec) splňovat požadavky článku 47 Listiny? Podle tohoto ustanovení má každý, jehož práva a svobody zaručené právem Unie byly porušeny, právo na účinné prostředky nápravy před soudem předem zřízeným zákonem.
218. Zatímco anglické znění článku 47 Listiny uvádí slovo „tribunal“, jiné jazykové verze dávají přednost slovu „soud“ (*court*)<sup>204</sup>. CDEU v rozsudku ve věci Schrems II zopakoval, že „procesním subjektům musí být dána možnost využít právních prostředků před nezávislým a nestranným soudem s cílem získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu těchto údajů“<sup>205</sup>. V témže kontextu posuzování odpovídající úrovně ochrany údajů se však SDEU domnívá, že účinnou soudní ochranu proti takovým zásahům může zajistit nejen soud, ale také orgán, který nabízí záruky v zásadě rovnocenné zárukám vyžadovaným v článku 47 Listiny<sup>206</sup>. EÚLP obdobně stanoví, že „každý, jehož práva a svobody přiznané touto Úmluvou byly porušeny, musí mít účinné opravné prostředky před národním orgánem“<sup>207</sup>, kterým, jak důsledně tvrdí ESLP, nemusí být nutně orgán soudní<sup>208</sup>. Pravomoci a procesní záruky, kterými určitý orgán disponuje, zejména to, zda je nezávislý na výkonné moci a zajišťuje spravedlivý proces, jsou naopak relevantní pro posouzení účinnosti tohoto prostředku nápravy před tímto orgánem<sup>209</sup>. Zdá se, že oba soudy nezakládají své posouzení na čistě formalistických kritériích, ale považují za rozhodující hmotněprávní záruky.
219. Ve věci Schrems II věnoval SDEU obzvláštní pozornost účinné ochraně v oblasti přístupu k osobním údajům z důvodů národní bezpečnosti. EDPB bere na vědomí, že SDEU přitom neprojednal prvek „předem zřízený zákonem“ v článku 47 Listiny, přestože mechanismus ombudsmana ve věcech štítu na ochranu soukromí rovněž nebyl založen na právních předpisech USA. Místo toho, aby se SDEU zabýval touto otázkou, posuzoval pro účely svého testu odpovídající ochrany různé aspekty, jako je například nedostatek pravomocí umožňujících zjednat nápravu. Rozsudek ve věci Schrems II tak

---

<sup>203</sup> Ustanovení § 5 písm. h) dekretu EO 14086 výslovně vytváří nárok subjektů údajů podávat stížnosti v souladu s mechanismem nápravy.

<sup>204</sup> Například „Gericht“ v německé jazykové verzi.

<sup>205</sup> Rozsudek SDEU ve věci Schrems II, bod 194.

<sup>206</sup> Rozsudek SDEU ve věci Schrems II, bod 197.

<sup>207</sup> Článek 13 EÚLP.

<sup>208</sup> Rozsudek ESLP ve věci Klass, bod 67; rozsudek ESLP ve věci Big Brother Watch, bod 359.

<sup>209</sup> Rozsudek ESLP ve věci Klass, bod 67; rozsudek ESLP ve věci Big Brother Watch, bod 359.

neposkytuje žádné vodítko pro posouzení pojmu „předem zřízený zákonem“ podle článku 47 Listiny. SDEU se však k této záležitosti vyjádřil i v jiných rozhodnutích. SDEU s odkazem na ustálenou judikaturu ESLP v tomto ohledu ve věcech C-487/19 a C-132/20 připomněl, že zavedení výrazu „předem zřízený zákonem“ má za cíl zabránit tomu, aby bylo uspořádání soudního systému v demokratické společnosti ponecháno na volném uvážení výkonné moci, a namísto toho zajistit, aby se tato oblast řídila zákonem přijatým zákonodárnou mocí způsobem, který je v souladu s pravidly upravujícími výkon její pravomoci<sup>210</sup>. Jak vyplývá z tohoto prohlášení, právo na soud „předem zřízený zákonem“ je velmi úzce spjato se zárukou nezávislosti.

220. V této souvislosti dospěl EDPB k závěru, že v kontextu posuzování odpovídající úrovně ochrany není zvláštní mechanismus nápravy vytvořený dekretem EO 14086 na rozdíl od nápravných opatření u soudů podle článku III sám o sobě nedostatečný. Analýza úrovně ochrany v tomto ohledu závisí na tom, zda záruky stanovené dekretem EO 14086 a doplněné nařízením ministra spravedlnosti dostatečně zajišťují nezávislost DPRC ve vztahu k ostatním orgánům.
221. Komise by měla průběžně sledovat, zda jsou pravidla stanovená v dekretu EO 14086 a jeho doplňujících ustanoveních, zejména ta, která mají podpořit nezávislost DPRC, plně prováděna a zda účinně fungují v praxi. Kromě toho by jakékoli změny tohoto rámce měly být pečlivě přezkoumány z hlediska dopadu na posouzení Komise podle návrhu rozhodnutí. V tomto ohledu EDPB konstatuje, že změny dekretu EO 14086 a nařízení ministra spravedlnosti mohou vést k přijetí okamžitě použitelných prováděcích aktů o pozastavení, zrušení nebo změně rozhodnutí o odpovídající ochraně<sup>211</sup>.

#### 3.2.4.2 Dostatečná nezávislost na výkonné moci

222. SDEU ve svém rozsudku ve věci Schrems II zdůraznil, že musí být zajištěna nezávislost daného soudu nebo orgánu, zejména na výkonné moci, včetně všech nezbytných záruk, a to i pokud jde o podmínky jeho odvolání nebo zrušení jmenování. SDEU konkrétně kritizoval skutečnost, že ombudsman byl ustanoven ministrem zahraničních věcí a byl mu přímo podřízen. Ombudsman byl považován za nedílnou součást ministerstva zahraničních věcí USA. SDEU rovněž konstatoval, že neexistují žádné zvláštní záruky pro odvolání nebo zrušení jmenování ombudsmana, což vyvolává pochybnosti o nezávislosti ombudsmana na výkonné moci.
223. EDPB uznává, že ustanovení dekretu EO 14086 a doplňkového nařízení ministra spravedlnosti neukládají soudu DPRC oznamovací povinnost vůči ministrovi spravedlnosti, jak by tomu bylo v případě vztahu nadřízenosti a podřízenosti. DPRC nepodléhá ani „každodennímu dohledu“ ministra spravedlnosti<sup>212</sup>. Tyto záruky představují významné zlepšení oproti štítu na ochranu soukromí. DPRC je však zřízen v rámci výkonné moci, konkrétně ministerstva spravedlnosti. Zejména z tohoto důvodu bude provádění a účinné fungování záruk v praxi rozhodující pro určení toho, zda lze DPRC považovat v praxi za dostatečně nezávislý i přesto, že sice není nedílnou součástí ministerstva spravedlnosti, ale je subjektem spadajícím pod výkonnou moc. EDPB vyzývá Komisi, aby pečlivě sledovala, zda se tyto záruky plně odrážejí v praxi. EDPB navíc navrhuje vyjasnit pojem „každodenní dohled“ tak, aby „soudci“ DPRC nepodléhali žádnému dohledu. Komise potvrdila, že pojem „každodenní dohled“ je třeba chápat v tomto smyslu.

<sup>210</sup> Viz SDEU, C-487/19, rozsudek ze dne 6. října 2021, W.Ž, ECLI:EU:C:2021:798 a C-132/20, rozsudek ze dne 29. března 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, bod 129 a bod 121.

<sup>211</sup> Návrh rozhodnutí, 212. bod odůvodnění.

<sup>212</sup> Nařízení ministra spravedlnosti, § 201.7(d).

224. Pokud jde o výše uvedené záruky, rámec EU-USA pro ochranu údajů předpokládá určité záruky týkající se jmenování a odvolávání „soudců“ DPRC. Ti jsou sice jmenováni ministrem spravedlnosti, ale jejich jmenování vychází z kritérií používaných pro hodnocení uchazečů o pozice federálních soudců a zahrnuje konzultaci s výborem PCLOB. Odvolání „soudců“ před uplynutím jejich funkčního období nebo z probíhajícího řízení je možné pouze za úzce vymezených okolností, které podle informací EDPB vycházejí z ustanovení vztahujících se na federálního soudce<sup>213</sup>. Uplatňování těchto pravidel představuje další krok k posílení nezávislého postavení DPRC, pro které bude opět mít zásadní význam jejich provádění v praxi. Z návrhu rozhodnutí jako takového však není jasné, zda a jak bude v USA dodržován soulad s těmito požadavky. EDPB na základě dodatečných vysvětlení poskytnutých Komisí a vládou USA vyrozuměl, že výbor PCLOB se může výše uvedenými ustanoveními zabývat v rámci svého každoročního přezkumu procesu nápravy, a že odpovědnost za monitorování a zajištění dodržování všech právních požadavků generálního inspektora v rámci ministerstva spravedlnosti zahrnuje požadavky uvedené v dekretu EO 14086 a v předpisech o zřízení DPRC. EDPB vyzývá Komisi, aby tento aspekt v návrhu rozhodnutí objasnila. Komise by však měla tyto záruky zohlednit při monitorování skutečné praxe zpracování osobních údajů, jak je posouzena v návrhu rozhodnutí.
225. Návrh rozhodnutí se nezabývá otázkou, zda, a pokud ano, za jakých podmínek, má prezident USA pravomoc propustit nebo odvolat „soudce“ DPRC. EDPB má za to, že taková pravomoc neexistuje, jak vysvětlila Evropská komise a potvrdili zástupci vlády USA. EDPB navrhuje tento aspekt v rozhodnutí o odpovídající ochraně vyjasnit.
226. „Soudci“ DPRC jsou jmenováni na čtyřletá funkční období, která lze prodloužit, a po dobu dvou let předcházejících jejich prvnímu jmenování nesmí být zaměstnáni v rámci výkonné moci<sup>214</sup>. Během doby, po kterou jsou jmenováni jako „soudci“ DPRC, nesmí mít žádné jiné oficiální povinnosti ani být zaměstnáni ve vládě USA<sup>215</sup>. Na rozdíl od federálních soudců USA se však mohou účastnit mimosoudních činností včetně obchodních činností, finančních činností, neziskových činností zabývajících se získáváním finančních prostředků, fiduciárních činností a poskytování právních služeb, pokud tyto činnosti nezasahují do nestranného výkonu jejich povinností nebo do účinnosti či nezávislosti DPRC<sup>216</sup>. Nezávislost soudnictví vyplývá nejen z nezávislosti na vnějších pokynech, ale také z osobní nezávislosti. V této souvislosti jsou relevantní faktory, jako je například funkční období, možnost být znovu jmenován a možnost střetu zájmů. Čtyřleté funkční období uvedené v dekretu EO 14086 a v nařízení ministra spravedlnosti je sice kratší než například funkční období soudců SDEU (šest let s možností opětovného jmenování) a ESLP (devět let bez možnosti opětovného jmenování), ale samo o sobě nevzbuzuje vážné obavy. EDPB si není vědom existence jakékoli judikatury, která by v tomto ohledu stanovovala minimální délku funkčního období<sup>217</sup>. EDPB rovněž uznává, že možnost zapojit se do mimosoudních činností je podmíněna tím, že jednoduše řečeno nepovede ke střetu zájmů, který by ohrozil povinnosti ve vztahu k DPRC. EDPB z dodatečných vysvětlení vlády USA vyrozuměl, že tyto požadavky rovněž podléhají přezkumu a monitorování ze strany výboru PCLOB a generálního inspektora Ministerstva spravedlnosti USA (viz bod 226 výše). V rámci společných přezkumů by měl být rovněž řešen způsob, jak bude tento požadavek uplatňován a prokazován v praxi.

---

<sup>213</sup> EO 14086, § 3(d)(iv); nařízení ministra spravedlnosti § 201.7.

<sup>214</sup> Nařízení ministra spravedlnosti § 201.3 (a).

<sup>215</sup> Nařízení ministra spravedlnosti § 201.3 (c).

<sup>216</sup> Nařízení ministra spravedlnosti § 201.7 (c).

<sup>217</sup> Viz rovněž obdobně rozsudek ESLP (Velkého senátu) ve věci Centrum För Rättvisa v. Švédsko ze dne 25. května 2021, bod 346.



227. Podle § 3(d)(i)(B) dekretu EO 14086 musí být všichni „soudci“ DPRC držitelé bezpečnostní prověrky, aby měli přístup k utajovaným informacím, tj. aby mohli vykonávat samotnou funkci rozhodování případů národní bezpečnosti<sup>218</sup>. Některé evropské předpisy o bezpečnostních prověrkách naopak soudce od tohoto požadavku na bezpečnostní prověrku osvobozují v rozsahu, v jakém vykonávají soudní funkce, neboť mají za to, že taková podrobná kontrola je potenciálně v rozporu s nezávislostí soudnictví<sup>219</sup>. Podle vysvětlení vlády USA sice kandidát na jmenování soudcem u soudu USA prochází důkladným prověřením, avšak federální soudce po svém jmenování federálním soudcem u soudu USA již nemá povinnost získat bezpečnostní prověrku pro přístup k utajovaným dokumentům relevantním pro daný případ.
228. Výše uvedené okolnosti podle názoru EDPB částečně odhalují rozdíly mezi postavením a statutem federálního soudce USA a „soudce“ DPRC. Poskytnuté záruky však nezavádějí důvod k pochybnostem o nezávislosti DPRC. EDPB naléhavě vyzývá Komisi, aby se v případě, že bude návrh rozhodnutí přijat, výše uvedené záruky staly prioritou při prvním společném přezkumu rámce EU-USA pro ochranu údajů. EDPB dále předpokládá, že pokud bude toto rozhodnutí přijato, dostojí Komise svému závazku je pozastavit, zrušit nebo změnit v případě, že by se výkonná moc USA rozhodla omezit záruky uvedené v dotyčném dekretu<sup>220</sup>.

### 3.2.4.3 Právomoci DPRC

#### 3.2.4.3.1 Přístup k informacím

229. Účinná právní ochrana vyžaduje, aby soud měl dostatečné vyšetřovací pravomoci k přezkumu napadeného opatření. SDEU ve věci Kadi II ve vztahu k článku 47 Listiny rozhodl, že unijní soud je povinen se ujistit, že se rozhodnutí opírá o dostatečně pevný skutkový základ<sup>221</sup>. SDEU konstatuje, že „unijní soud musí v rámci tohoto přezkumu za tímto účelem případně vyzvat příslušný unijní orgán, aby předložil důvěrné i nedůvěrné informace a důkazy, které jsou pro takový přezkum relevantní“<sup>222</sup>, přičemž „nelze namítat tajnost nebo důvěrnost [...] informací nebo důkazů“<sup>223</sup>.
230. Podle 181. bodu odůvodnění návrhu rozhodnutí DPRC přezkoumává rozhodnutí CLPO přinejmenším na základě záznamů o vyšetřování CLPO, jakož i veškerých informací a podání poskytnutých stěžovatelem, zvláštním advokátem nebo zpravodajskou službou. Návrh rozhodnutí dále uvádí, že DPRC má přístup ke všem nezbytným informacím, které může získat prostřednictvím CLPO. To je založeno na ustanovení § 201.9 písm. b) nařízení ministra spravedlnosti, které opravňuje DPRC „požadovat, aby CLPO doplnil záznam o konkrétní vysvětlující nebo objasňující informace a aby v případě potřeby provedl další faktická zjištění nezbytná k tomu, aby panel DPRC mohl provést přezkum“. EDPB má za to, že posouzení provedené DPRC se tedy v žádném případě neomezuje na zjištění CLPO na první úrovni nového mechanismu nápravy. DPRC si naopak může vyžádat jak dodatečné právní informace, tak především další skutkové okolnosti pro účely analýzy toho, zda došlo k porušení v dané oblasti působnosti. EDPB zároveň konstatuje, že tyto obecně rozsáhlé vyšetřovací pravomoci se nevztahují na přímý přístup k uchovávaným údajům o dané fyzické osobě. Komise objasnila, že pokud bude DPRC požadovat další informace, bude CLPO vždy fungovat jako

<sup>218</sup> Viz rovněž nařízení ministra spravedlnosti § 201.11 (b) a návrh rozhodnutí, 177. bod odůvodnění.

<sup>219</sup> Např. § 2 odst. 3 německého zákona o bezpečnostních prověrkách.

<sup>220</sup> Návrh rozhodnutí, 212. bod odůvodnění.

<sup>221</sup> SDEU, spojené věci C-584/10P, C-593/10P a C-595/10P, Evropská komise a další v. Yassin Abdullah Kadi, rozsudek ze dne 18. července 2013 (dále jen „rozsudek SDEU ve věci Kadi II“), bod 119.

<sup>222</sup> Rozsudek SDEU ve věci Kadi II, bod 120.

<sup>223</sup> Rozsudek SDEU ve věci Kadi II, bod 125.

zprostředkovatel. Přístup DPRC k informacím nezbytným k nezávislému rozhodování o žádosti o přezkum proto do jisté míry závisí na tom, zda CLPO poskytne potřebné informace. EDPB uznává, že CLPO má povinnost poskytnout DPRC „veškerou nezbytnou podporu“ a zpravodajské agentury jsou povinny poskytnout kanceláři CLPO přístup k informacím nezbytným k provedení přezkumu soudem DPRC<sup>224</sup>. EDPB však rovněž konstatuje, že kancelář CLPO sama není nezávislá a že provádí počáteční šetření stížnosti v první fázi postupu pro zajištění nápravy. EDPB proto vítá, že výbor PCLOB během svých každoročních přezkumů nápravného mechanismu ověří, zda DPRC získal neomezený přístup ke všem nezbytným informacím<sup>225</sup>. EDPB dále vyzývá Komisi, aby tento aspekt zahrnula do společných přezkumů, bude-li návrh rozhodnutí přijat, s cílem přezkoumat dopady tohoto systému v praxi.

#### *3.2.4.3.2 Právomoci umožňující zjednat nápravu*

231. Jedním z hlavních nedostatků štítu na ochranu soukromí, který vedl k tomu, že ho SDEU ve věci Schrems II prohlásil za neplatný, byl nedostatek závazných pravomocí ombudsmana umožňujících zjednat nápravu. SDEU konstatoval, že „řešené rozhodnutí neobsahuje žádnou zmínku o tom, že by tento ombudsman měl pravomoc přijímat závazná rozhodnutí ve vztahu k této [zpravodajské] komunitě“<sup>226</sup>. Pouhý (politický) závazek vlády USA v tom smyslu, že zpravodajská komunita napraví každé nedodržení příslušných předpisů zjištěné ombudsmanem, nebyla postačující k zajištění úrovně ochrany, která by byla v zásadě rovnocenná úrovni ochrany zaručené článkem 47 Listiny.
232. V rámci nového nápravného mechanismu mají naopak rozhodnutí přijatá CLPO a DPRC závazný účinek<sup>227</sup>. EDPB na jedné straně uznává, že tato pravomoc není omezena na konkrétní opatření, ale umožňuje „náležitou nápravu“ s cílem zajistit „úplnou nápravu“ zjištěného porušení. Zejména § 4 písm. a) dekretu EO 14086 výslovně zmiňuje výmaz protiprávně shromážděných údajů. EDPB na druhou stranu poznamenává, že znění § 4 písm. a) dekretu EO 14086 vytváří určitou nejistotu, pokud jde o proces určení takové „náležité nápravy“. Opatření by sice měla být navržena tak, aby bylo dosaženo plné nápravy porušení předpisů, je však třeba přihlídnout i ke „způsobům, jakými se zjištěná porušení podobného druhu řeší obvykle“<sup>228</sup>. Význam a účinek tohoto požadavku je nejasný. EDPB proto vyzývá Komisi, aby úzce monitorovala nápravná opatření přijatá v praxi.

#### *3.2.4.4 Podání stížnosti v rámci nového mechanismu nápravy*

233. Mechanismus nápravy zavedený podle dekretu EO 14086 se vztahuje pouze na způsobilé stížnosti podané příslušným veřejným orgánem ve způsobilém státě ve vztahu k činnostem signálového zpravodajství USA ohledně jakéhokoli porušení v příslušné oblasti působnosti<sup>229</sup>. Aby bylo možné využít této právní ochrany, musí být proto splněno několik podmínek.

##### *3.2.4.4.1 Označení jako způsobilý stát*

234. Za prvé, země nebo organizace regionální hospodářské integrace, odkud byly údaje předány do USA, musí být před předáním údajů, na nichž je daná stížnost založena, označena za způsobilý stát<sup>230</sup>. Zjevně je nezbytné, aby byl daný mechanismus nápravy k dispozici v okamžiku, kdy vstoupí v platnost dané rozhodnutí o odpovídající ochraně. 196. bod odůvodnění návrhu rozhodnutí proto stanoví, že vstup

<sup>224</sup> EO 14086, § 3(c)(i)(H) a § 3(d)(iii).

<sup>225</sup> EO 14086, § 3(e)(i).

<sup>226</sup> Rozsudek SDEU ve věci Schrems II, bod 196.

<sup>227</sup> EO 14086, § 3(c)(ii) a § 3(d)(ii).

<sup>228</sup> EO 14086, § 4(a).

<sup>229</sup> EO 14086, § 3(a).

<sup>230</sup> EO 14086, § 4(d)(i) a § 4(k)(i).

rozhodnutí v platnost je podmíněn mimo jiné určením Unie jako kvalifikovaného subjektu pro účely tohoto mechanismu. Komise totiž pravděpodobně předpokládá, že k tomuto určení dojde před přijetím rozhodnutí, neboť návrh již obsahuje zástupný symbol pro pověření EU ministrem spravedlnosti USA<sup>231</sup> (na rozdíl od zahrnutí tohoto pověření jako odkládací podmínky do výroku návrhu rozhodnutí).

#### 3.2.4.4.2 *Nepříznivý dopad na zájmy v oblasti soukromí a občanských svobod a „legitimaci“*

235. „Způsobilá stížnost“ musí být založena na údajném „porušení v příslušné oblasti působnosti“, což zase předpokládá porušení, které nepříznivě ovlivňuje individuální zájmy stěžovatele v oblasti soukromí a občanských svobod<sup>232</sup>. Na základě dodatečných vysvětlení Komise má EDPB za to, že výraz „nepříznivě ovlivňuje“ neznamená žádnou formu omezení přípustnosti stížnosti. Jak Komise uvedla, takový nepříznivý dopad by se vztahoval spíše na veškeré stížnosti týkající se zpracování osobních údajů pro účely činností signálového zpravodajství v rozporu s ustanoveními uvedenými v § 4(d)(iii), např. se zárukami dekretu EO 14086. EDPB vyjadřuje politování nad tím, že tato skutečnost není v textu návrhu rozhodnutí upřesněna, a vyzývá Komisi, aby dále vyjasnila pojem „nepříznivé ovlivnění“ s cílem zajistit, aby byla posouzena a napravena veškerá porušení práv subjektů údajů a aby nebylo za účelem přístupu k nápravným opatřením a náležité nápravě nutno prokazovat žádnou úroveň „závažnosti“.
236. Jak již bylo uvedeno, stížnost podle dekretu EO 14086 nevyžaduje, aby žalobce prokázal aktivní legitimaci (viz bod 215)<sup>233</sup>. EDPB vítá vyjasnění v § 4 písm. k) dekretu EO 14086, že se použije test „důvodné domněnky“ a že není nutné prokázat, že údaje stěžovatele byly skutečně zpřístupněny prostřednictvím signálních zpravodajských činností. Zřízení nápravného mechanismu je důležitým krokem, neboť požadavek týkající se legitimace velmi ztěžuje napadnutí opatření dohledu před běžnými soudy v USA.
237. Na základě výše uvedených skutečností se EDPB nedomnívá, že by bylo možné při obrácení se na běžné soudy, na něž návrh rozhodnutí rovněž odkazuje<sup>234</sup>, poskytnout odpovídající úroveň ochrany<sup>235</sup>. V tomto ohledu EDPB připomíná své obavy, které již mnohokrát vyjádřil v souvislosti s požadavkem na aktivní legitimaci před běžnými soudy<sup>236</sup>. Kromě toho má EDPB na základě dodatečných prohlášení vlády USA za to, že ačkoli dekret EO 14086 nevylučuje odvolání k soudům s obecnou příslušností, není jisté, jak by takový soud tento dekret uplatnil. Pokud bude návrh rozhodnutí přijat, bylo by možno se touto otázkou dále zabývat v budoucích přezkumech.

#### 3.2.4.4.3 *Postup při podávání stížnosti*

238. EDPB v zásadě schvaluje postup předávání stížnosti prostřednictvím dozorových úřadů členských států, a je i nadále přesvědčen, že zjištění totožnosti stěžovatele by mělo být provedeno na území EU. Stejně jako v rámci mechanismu ombudsmana ve věcech štítu na ochranu soukromí však návrh rozhodnutí stanoví, že subjekt údajů, který chce takovou stížnost podat, ji musí předložit dozorovému úřadu v členském státě EU příslušnému pro dohled nad národními bezpečnostními službami a/nebo pro zpracování osobních údajů orgány veřejné moci<sup>237</sup>. V tomto ohledu připomíná EDPB své obavy

<sup>231</sup> Návrh rozhodnutí, poznámka pod čarou 320.

<sup>232</sup> EO 14086, § 4(k)(i) a 4(d)(ii).

<sup>233</sup> Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II., s. 10.

<sup>234</sup> Návrh rozhodnutí, 187. a následující body odůvodnění.

<sup>235</sup> Viz rovněž rozsudek SDEU ve věci Schrems II, body 191 a 192.

<sup>236</sup> Viz stanovisko skupiny WP 29 č. 1/2016, s. 43.

<sup>237</sup> Návrh rozhodnutí, 169. bod odůvodnění.

vyjádřené již ve stanovisku pracovní skupiny zřízené podle článku 29 ke štítu na ochranu soukromí, například potenciální obtíže fyzických osob při určování příslušného orgánu vzhledem k různorodosti mechanismů dohledu nad národními bezpečnostními službami v členských státech<sup>238</sup>. S ohledem na zapojení vnitrostátních orgánů pro ochranu údajů při uplatňování rámce EU-USA pro ochranu údajů a dohledu nad ním je vhodnější podávat stížnosti prostřednictvím těchto orgánů.

#### 3.2.4.5 Rozhodnutí DPRC

239. Po dokončení přezkumu žádosti stěžovatele nesmí DPRC sdělit, zda byl stěžovatel subjektem činností signálového zpravodajství USA. Namísto toho je stěžovatel upozorněn, že „přezkum buď nezjistil žádná porušení v dané oblasti působnosti, nebo DPRC vydal rozhodnutí vyžadující náležitou nápravu“<sup>239</sup>. Tato standardní odpověď slouží obecně legitimnímu účelu ochrany citlivých informací o zpravodajských činnostech USA. EDPB je však znepokojen tím, že dekret EO 14086 nestanoví z této standardní odpovědi DPRC žádné výjimky.
240. Ve věci Kadi II se SDEU musel zabývat protichůdnými zájmy státního tajemství na jedné straně a spravedlivým a pokud možno kontradiktorním řízením na straně druhé. SDEU rozhodl, že za okolností, kdy bezpečnostní imperativy nebo důvody spojené s vnitrostátní bezpečností brání sdělení určitých informací nebo důkazů dotyčné osobě, je úkolem soudu, aby v rámci soudního přezkumu použil techniky, které umožňují skloubit legitimní bezpečnostní zájmy týkající se povahy a zdroje informací s nutností zaručit jednotlivcům v dostatečné míře dodržování jejich procesních práv, jako jsou právo být vyslechnut či zásada kontradiktornosti<sup>240</sup>. SDEU dále upřesnil, že soud musí za tímto účelem v rámci přezkumu všech právních a skutkových okolností uváděných příslušným unijním orgánem ověřit, zda jsou důvody uplatňované uvedeným orgánem k zabránění takovému sdělení podloženy<sup>241</sup>. Jeví-li se, že důvody uváděné příslušným unijním orgánem skutečně brání tomu, aby byly dotyčné osobě sděleny informace nebo důkazy, je i nadále nutné odpovídajícím způsobem vyvážit požadavky týkající se práva na účinnou soudní ochranu, a požadavky týkající se vnitrostátní bezpečnosti<sup>242</sup>. Za účelem nastolení takové rovnováhy lze využít možností, jako je sdělení shrnutí obsahu dotčených informací nebo důkazů<sup>243</sup>. Ačkoli zjištění soudu neukládají požadavky na rozhodnutí vydané soudem, ale týkají se spíše rozhodnutí příslušného orgánu a vedení soudního řízení, poskytují údaje o vyvážení výše uvedených zájmů v souvislosti s právem na účinnou právní ochranu. Pro další orientaci lze odkázat rovněž na věc Big Brother Watch, kdy ESLP s odkazem na spravedlivost řízení a zejména na zásadu kontradiktornosti rozhodl, že rozhodnutí soudního nebo jinak nezávislého orgánu by měla být odůvodněná<sup>244</sup>.
241. EDPB uznává, že rozhodnutí DPRC jsou skutečně odůvodněná. DPRC je výslovně povinen vydat písemné rozhodnutí, v němž uvede svá zjištění a specifikaci jakékoli náležité nápravy<sup>245</sup>. EDPB navíc uvádí, že pokud budou informace týkající se přezkumu ze strany DPRC odtajněny, bude to dané fyzické osobě oznámeno<sup>246</sup>. EDPB rovněž uznává úlohu zvláštních advokátů předpokládanou v novém nápravném mechanismu, která zahrnuje obhajobu zájmů stěžovatele v dané věci<sup>247</sup>. S ohledem na výše uvedené

<sup>238</sup> Stanovisko skupiny WP 29 č. 1/2016, s. 48 a 49.

<sup>239</sup> EO 14086, § 3(d)(i)(H). Ustanovení dekretu EO 14086 stanoví tuto odpověď i pro CLPO.

<sup>240</sup> Rozsudek SDEU ve věci Kadi II, bod 125.

<sup>241</sup> Rozsudek SDEU ve věci Kadi II, bod 126.

<sup>242</sup> Rozsudek SDEU ve věci Kadi II, bod 128.

<sup>243</sup> Rozsudek SDEU ve věci Kadi II, bod 129.

<sup>244</sup> Rozsudek ESLP ve věci Big Brother Watch, bod 359.

<sup>245</sup> Nařízení ministra spravedlnosti, § 201.9(g).

<sup>246</sup> EO 14086, § 3(d)(v).

<sup>247</sup> Nařízení ministra spravedlnosti, § 201.8(g).

důsledky judikatury SDEU a ESLP a na to, že proti rozhodnutí DPRC se nelze odvolat, ale je konečné<sup>248</sup>, však má EDPB obavy ohledně obecného uplatňování standardní reakce DPRC. EDPB připomíná, že výbor PCLOB nezávisle přezkoumá fungování nového nápravného mechanismu, a vyzývá Komisi, aby této otázce věnovala zvláštní pozornost, včetně jakéhokoli posouzení tohoto aspektu výborem PCLOB během budoucích přezkumů tohoto rozhodnutí v případě, že bude přijato.

## 4 PROVÁDĚNÍ A MONITOROVÁNÍ NÁVRHU ROZHODNUTÍ

242. Pokud jde o monitorování a přezkum návrhu rozhodnutí, EDPB konstatuje, že podle judikatury SDEU „s ohledem na skutečnost, že se úroveň ochrany zajišťovaná třetí zemí může vyvíjet, je na Komisi, aby po přijetí rozhodnutí o odpovídající úrovni ochrany na základě [článku 45 GDPR] pravidelně ověřovala, zda zjištění ohledně odpovídající úrovně ochrany zajišťované dotyčnou třetí zemí je stále skutkově a právně podložené. Takové ověřování je každopádně závazné tehdy, když některé indicie vyvolávají v tomto ohledu určité pochybnosti“<sup>249</sup>.
243. EDPB navíc konstatuje, že dopis ministerstva obchodu stanoví, že ministerstvo obchodu a popřípadě další agentury USA budou pravidelně pořádat zasedání s Komisí, zúčastněnými orgány pro ochranu údajů z EU a příslušnými zástupci EDPB<sup>250</sup>.
244. EDPB má za to, že v průběhu příštích pravidelných přezkumů si zaslouží zvláštní pozornost ochrana podle státního práva ve vztahu k přístupu donucovacích orgánů, výjimka pro dočasné hromadné shromažďování s ohledem na cílené shromažďování vnitrostátními bezpečnostními orgány USA, uplatňování nově zavedených zásad nezbytnosti a přiměřenosti v praxi, a to i v souvislosti s programem UPSTREAM, vzájemné působení mezi dekretem EO 14086 a různými právními nástroji USA, které umožňují zpravodajským službám USA shromažďovat a dále zpracovávat osobní údaje, prováděcí vnitřní politiky a postupy, způsob, jakým budou tyto záruky rovněž zohledněny v souvislosti s dohledem vedeným soudem FISC a jak bude účinně fungovat nápravný mechanismus, a otázka dalšího předávání, automatizovaná rozhodnutí, věcný a účinný dohled a prosazování zásad rámce pro ochranu údajů, jakož i účinná nápravná opatření.
245. EDPB konstatuje, že přezkum zjištění o odpovídající ochraně se uskuteční po jednom roce od data oznámení rozhodnutí o odpovídající ochraně členskými státy a následně nejméně každé čtyři roky<sup>251</sup>. S cílem dále posílit průběžné monitorování rozhodnutí o odpovídající ochraně vyzývá EDPB Komisi, aby následné přezkumy prováděla alespoň každé tři roky.
246. Pokud jde o praktické zapojení EDPB a jeho zástupců do přípravy a provádění budoucích pravidelných přezkumů, EDPB opakuje, že veškerá příslušná dokumentace včetně korespondence by měla být s EDPB sdílena písemně s dostatečným předstihem před provedením přezkumů. Stejně jako v případě přezkumů prováděných v rámci štítu na ochranu soukromí EDPB doporučuje, aby byly nejpozději tři měsíce před konáním přezkumu stanoveny a dohodnuty způsoby přezkumu mezi Komisí, administrativou USA a EDPB.
247. EDPB dále bere na vědomí a vítá skutečnost, že 212. bod odůvodnění návrhu rozhodnutí uvádí příklady změn narušujících úroveň ochrany, které mohou odůvodnit zahájení „nouzového postupu zrušení“

---

<sup>248</sup> Nařízení ministra spravedlnosti, § 201.9(g).

<sup>249</sup> Rozsudek SDEU ve věci Schrems I, bod 76. Viz rovněž návrh rozhodnutí, čl. 3 odst. 4.

<sup>250</sup> Návrh rozhodnutí, příloha III.

<sup>251</sup> Návrh rozhodnutí, čl. 3 odst. 4.

zaměřeného na změny, k nimž by mohlo dojít v souvislosti s dekretem 14086 a se souvisejícím nařízením ministra spravedlnosti.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)