



18/CS

WP 254 rev. 01

Pracovní skupina zřízená podle článku 29

Referenční rámec pro odpovídající ochranu

Přijato dne 28. listopadu 2017

V posledním znění přijatém dne 6. února 2018

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Služby sekretariátu zajišťuje ředitelství C (Základní práva a občanství Unie) Evropské komise, Generální ředitelství pro spravedlnost, B-1049, Brusel, Belgie, kancelář MO-59 02/013.

Internetové stránky: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Úvod

Pracovní skupina orgánů EU pro ochranu údajů¹ (dále jen „skupina WP29“) dříve zveřejnila pracovní dokument o předávání osobních údajů do třetích zemí (WP12).² Po nahrazení směrnic obecným nařízením EU o ochraně údajů³ se skupina WP29 k dokumentu WP12 vrací, aby své předchozí pokyny přepracovala v kontextu nové právní úpravy a nedávné judikatury Soudního dvora EU⁴.

Smyslem tohoto pracovního dokumentu je aktualizovat první kapitolu dokumentu WP12, která upravuje ústřední otázku odpovídající úrovně ochrany údajů ve třetí zemi, na určitém území nebo v jednom či více konkrétních odvětvích v této třetí zemi anebo v mezinárodní organizaci (dále jen: „třetí země nebo mezinárodní organizace“). Tento dokument bude v následujících letech průběžně revidován a v případě potřeby aktualizován na základě praktických zkušeností získaných při uplatňování obecného nařízení o ochraně osobních údajů. Později by měly být aktualizovány kapitoly 2 (*Uplatňování přístupu v zemích, které ratifikovaly úmluvu č. 108*) a 3 (*Uplatňování přístupu v oblastí samoregulace průmyslu*) dokumentu WP12.

Tento pracovní dokument se soustředí výhradně na rozhodnutí o odpovídající ochraně, kterými se provádějí akty⁵ Evropské komise podle článku 45 obecného nařízení o ochraně osobních údajů. Jiné aspekty předávání osobních údajů do třetích zemí a mezinárodním organizacím budou přezkoumány v následujících pracovních dokumentech, které budou zveřejněny samostatně (závazná podniková pravidla, odchylky).

Cílem tohoto dokumentu je stanovit základní zásady ochrany údajů, které musí právní rámec třetí země nebo mezinárodní organizace obsahovat, aby byl v zásadě rovnocenný rámci EU, a poskytnout tak v rámci obecného nařízení o ochraně osobních údajů Evropské komisi a skupině WP29 pokyny k posuzování úrovně ochrany údajů ve třetích zemích a mezinárodních organizacích. Dokument může sloužit také jako vodítko pro třetí země a mezinárodní organizace, které usilují o dosažení odpovídající ochrany. Zásady vytyčené v tomto pracovním dokumentu však nejsou určeny přímo správcům ani zpracovatelům údajů.

Tento dokument je rozdělen do 4 kapitol:

Kapitola 1: Některé obecné informace související s konceptem odpovídající úrovně ochrany

Kapitola 2: Procesní aspekty závěrů ohledně odpovídající ochrany dle obecného nařízení o ochraně osobních údajů

Kapitola 3: Obecné zásady ochrany údajů. Tato kapitola obsahuje základní obecné zásady ochrany údajů, na jejichž základě lze ve třetí zemi nebo mezinárodní organizaci zajistit úroveň ochrany v zásadě rovnocennou úrovni stanovené právními předpisy EU.

Kapitola 4: Základní záruky přístupu pro účely prosazování práva a národní bezpečnosti, kterými se omezuje zásah do základních práv. Tato kapitola zahrnuje základní záruky přístupu k údajům pro účely prosazování práva a národní bezpečnosti na základě rozsudku Soudního dvora EU z roku 2015 ve věci Schrems a na základě dokumentu skupiny WP29 o základních zárukách přijatém v roce 2016.

¹Skupina byla zřízena podle článku 29 směrnice EU o ochraně údajů 95/46/ES.

² WP12 „Pracovní dokument: předávání osobních údajů do třetích zemí: uplatnění článků 25 a 26 směrnice EU o ochraně údajů“, který pracovní skupina přijala dne 24. července 1998.

³ 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) (Text s významem pro EHP).

⁴ Včetně věci C-362/14, Maximilian Schrems proti Data Protection Commissioner, 6. října 2015.

⁵ Další informace o prováděcích aktech jsou k dispozici v příslušných ustanoveních čl. 45 odst. 3 a čl. 93 odst. 2 obecného nařízení o ochraně osobních údajů.

Kapitola 1: Některé obecné informace související s konceptem odpovídající úrovně ochrany

Ustanovení čl. 45 odst. 1 obecného nařízení o ochraně osobních údajů vytyčuje zásadu, že předání údajů do třetí země nebo mezinárodní organizaci se může uskutečnit, jen pokud tato třetí země, území nebo jedno či více konkrétních odvětví v této třetí zemi anebo mezinárodní organizace zajišťují odpovídající úroveň ochrany.

Tento koncept „odpovídající úrovně ochrany“, který existoval již ve směrnici 95/46, byl dále rozpracován Soudním dvorem EU. Zde je nutné připomenout standard stanovený Soudním dvorem ve věci Schrems, konkrétně zásadu, že „úroveň ochrany“ ve třetí zemi musí být „v zásadě rovnocenná“ úrovni zaručované v EU, i když se „prostředky, které tato třetí země využívá v tomto směru k zajištění takovéto úrovně ochrany, mohou lišit od prostředků zavedených v rámci Unie“⁶. Cílem tedy není kopírovat legislativu EU krok za krokem, nýbrž stanovit základní, klíčové požadavky této legislativy.

Účelem rozhodnutí Evropské komise o odpovídající ochraně je formálně potvrdit⁷, že úroveň ochrany údajů ve třetí zemi nebo mezinárodní organizaci je v zásadě rovnocenná úrovni ochrany údajů v Evropské unii⁸, přičemž toto potvrzení má závazné účinky na členské státy. Odpovídající ochrana lze dosáhnout kombinací práv subjektů údajů a povinností subjektů, které údaje zpracovávají nebo nad takovým zpracováním a nad dohledem prováděným nezávislými orgány vykonávají kontrolu. Pravidla ochrany údajů jsou však účinná jen tehdy, jsou-li vymahatelná a uplatňována v praxi. Je tedy nutné přihlížet nejen k obsahu pravidel pro předávání osobních údajů 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.

V ustanovení čl. 45 odst. 2 obecného nařízení o ochraně osobních údajů jsou uvedeny prvky, které Komise vezme v úvahu při posuzování odpovídající úrovně ochrany ve třetí zemi nebo mezinárodní organizaci.

Komise například vezme v úvahu právní stát, dodržování lidských práv a základních svobod, příslušné právní předpisy, existenci a účinné fungování jednoho nebo více nezávislých dozorových úřadů a mezinárodní závazky, které daná třetí země nebo mezinárodní organizace přijala.

Je tedy zřejmé, že každá smysluplná analýza přiměřenosti ochrany musí zahrnovat dva základní prvky: obsah příslušných pravidel a prostředky k zajištění jejich účinného uplatňování. Je na Evropské komisi, aby pravidelně ověřovala, že zavedená pravidla jsou v praxi účinná.

„Hlavní“ zásady ochrany údajů týkající se „obsahu“ a požadavky na „procesní/donucovací“ mechanismy, které lze považovat za minimální požadavky na zajištění odpovídající ochrany, jsou odvozeny z Listiny základních práv Evropské Unie a z obecného nařízení o ochraně osobních údajů. Dále by se měly zohlednit další mezinárodní smlouvy o ochraně údajů, například úmluva č. 108⁹.

Pozornost je třeba věnovat také právnímu rámci pro zajištění přístupu veřejných orgánů k osobním údajům. V tomto ohledu poskytuje další pokyny pracovní dokument č. 237 (tj. dokument o základních zárukách)¹⁰ o ochranných opatřeních v souvislosti s dozorem.

Obecná ustanovení o ochraně údajů a soukromí ve třetí zemi nepostačují. Naopak, právní rámec třetí země nebo mezinárodní organizace musí zahrnovat konkrétní ustanovení upravující specifické potřeby u aspektů práva na ochranu údajů významných z praktického hlediska. Tato ustanovení musí být vymahatelná.

Kapitola 2: Procesní aspekty závěrů ohledně odpovídající ochrany dle obecného nařízení o ochraně osobních údajů

⁶ Věc C-362/14, Maximilian Schrems proti Data Protection Commissioner, 6. října 2015 (odstavce 73, 74).

⁷ Článek 288 (2) SFEU.

⁸ Věc C-362/14, Maximilian Schrems proti Data Protection Commissioner, 6. října 2015 (odstavec 52).

⁹ 105. bod odůvodnění obecného nařízení o ochraně osobních údajů.

¹⁰ Pracovní dokument č. 01/2016 o odůvodnění zásahů do základních práv na ochranu údajů a soukromí prostřednictvím opatření dozoru při předávání osobních údajů (Evropské základní záruky), 16/EN WP 237, 13. dubna 2016.

Aby mohla Evropská rada pro ochranu údajů plnit svůj úkol v oblasti poskytování poradenství Evropské komisi podle ustanovení čl. 70 odst. 1 písm. s) obecného nařízení o ochraně osobních údajů, musí mít k dispozici náležitou dokumentaci, včetně příslušné korespondence a zjištění učiněných Evropskou komisí. Je-li právní rámec složitý, měla by dokumentace zahrnovat veškeré zprávy vypracované na téma úrovně ochrany v příslušné třetí zemi nebo mezinárodní organizaci. V každém případě by informace poskytnuté Evropskou komisí měly být úplné a umožňovat Evropské radě pro ochranu údajů provést vlastní posouzení ochrany údajů ve třetí zemi. Evropská rada pro ochranu údajů včas poskytne stanovisko k závěrům Evropské komise a informuje o případných nedostatcích rámce pro zajištění odpovídající ochrany. Evropská rada pro ochranu údajů se také vynasnaží navrhnout změny nebo úpravy, kterými by se nedostatky daly řešit.

Podle ustanovení čl. 45 odst. 4 obecného nařízení o ochraně osobních údajů je na Evropské komisi, aby průběžně sledovala vývoj, který by mohl ovlivnit fungování přijatých rozhodnutí o odpovídající ochraně.

Podle ustanovení čl. 45 odst. 3 obecného nařízení o ochraně osobních údajů je nutné nejméně každé čtyři roky provést pravidelný přezkum. Tento obecný časový rámec je však třeba individuálně upravit u každé země či mezinárodní organizace, u níž bylo rozhodnuto o odpovídající ochraně. Za určitých okolností mohou existovat důvody pro stanovení kratšího cyklu přezkumu. Také incidenty nebo jiné informace vztahující se k právnímu rámci či změny v právním rámci třetí země nebo mezinárodní organizace si mohou vyžádat přezkum před plánovaným termínem. Rovněž se jeví jako vhodné provádět první přezkum zcela nového rozhodnutí o odpovídající ochraně relativně brzy a dle jeho výsledků cyklus přezkumu upravit.

Protože Evropská rada pro ochranu údajů má mandát předat Evropské komisi stanovisko ohledně toho, že daná třetí země, určité území nebo jedno či více konkrétních odvětví v této zemi nebo mezinárodní organizace již odpovídající ochranu nezajišťují, je nutné, aby včas obdržela smysluplné informace o sledování příslušného vývoje ve třetí zemi nebo mezinárodní organizaci prováděném Evropskou komisí. Proto by Evropská rada pro ochranu údajů měla být průběžně informována o všech procesech přezkumu a přezkumných misích ve třetí zemi nebo mezinárodní organizaci. Evropská rada pro ochranu údajů uvítá, bude-li přizvána, aby se takových přezkumných procesů a misí zúčastnila.

Je také třeba poznamenat, že podle ustanovení čl. 45 odst. 5 obecného nařízení o ochraně osobních údajů má Evropská komise právo stávající rozhodnutí o odpovídající ochraně zrušit, změnit nebo pozastavit. Do procesu zrušení, změny či pozastavení by pak měla být zapojena Evropská rada pro ochranu údajů, která by měla být požádána o vydání stanoviska podle ustanovení čl. 70 odst. 1 písm. s).

Podle ustanovení čl. 58 odst. 5 obecného nařízení o ochraně osobních údajů a rozsudku Soudního dvora ve věci Schrems navíc platí, že orgány pro ochranu údajů musí mít možnost zapojit se do soudních projednávání, považují-li za opodstatněnou výtku určité osoby vůči rozhodnutí o odpovídající ochraně: „*V tomto ohledu přísluší vnitrostátnímu normotvůrci, aby stanovil procesní prostředky, které by dotyčnému vnitrostátnímu orgánu dozoru umožnily uplatnit výtky, jež považuje za opodstatněné, před vnitrostátními soudy, aby tyto soudy v případě, že sdílí pochybnosti vyjádřené tímto orgánem ohledně platnosti rozhodnutí Komise, předložily žádost o rozhodnutí o předběžné otázce za účelem přezkumu platnosti tohoto rozhodnutí*“¹¹.

¹¹ Věc C-362/14, Maximilian Schrems proti Data Protection Commissioner, 6. října 2015 (odstavec 65).

Kapitola 3: Obecné zásady ochrany údajů, na jejichž základě lze ve třetí zemi, na určitém území nebo v jednom či více konkrétních odvětví v této třetí zemi nebo v mezinárodní organizaci zajistit úroveň ochrany v zásadě rovnocennou úrovni stanovené právními předpisy EU

Systém třetí země nebo mezinárodní organizace musí v oblasti ochrany údajů obsahovat následující základní obsahové, procesní a donucovací zásady a mechanismy:

A. Zásady ohledně obsahu:

1) Koncepty

Měly by existovat základní koncepty resp. zásady ochrany dat. Není nutné, aby kopírovaly terminologii obecného nařízení o ochraně osobních údajů, měly by však odpovídat a vyhovovat konceptům zakotveným v evropských právních předpisech o ochraně údajů. Obecné nařízení o ochraně osobních údajů obsahuje mimo jiné následující důležité koncepty: „osobní údaje“, „zpracování osobních údajů“, „správce údajů“, „zpracovatel údajů“, „příjemce“ a „citlivé osobní údaje“.

2) Odůvodnění zákonného a korektního zpracování k legitimním účelům

Údaje se musí zpracovávat zákonně, korektně a legitimně.

Legitimní základ, který umožňuje zákonné, korektní a legitimní zpracování osobních údajů, by měl být definován dostatečně jasně. Evropský rámec uznává několik takovýchto legitimních základů, včetně ustanovení vnitrostátního práva, souhlasu subjektu údajů, plnění smlouvy a oprávněných zájmů správce údajů nebo třetí strany, které nepřevažují nad zájmy jednotlivce.

3) Zásada účelového omezení

Údaje by se měly zpracovávat ke konkrétnímu účelu a následně používat jen tehdy, není-li to neslučitelné s účelem zpracování.

4) Zásada kvality údajů a přiměřenosti

Údaje by měly být přesné a v případě potřeby aktualizované. Osobní údaje by měly být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány.

5) Zásada uchovávání údajů

Údaje by se zpravidla neměly uchovávat déle, než je nezbytné pro účely, k nimž jsou zpracovávány.

6) Zásada zabezpečení a důvěrnosti

Všechny subjekty zpracovávající údaje by měly zajistit zpracování údajů způsobem, který za pomoci vhodných technických nebo organizačních opatření zajišťuje zabezpečení osobních údajů, včetně ochrany před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Úroveň zabezpečení je třeba posuzovat s ohledem na stav techniky a související náklady.

7) Zásada transparentnosti

Každý by měl být informován o všech hlavních aspektech zpracování svých osobních údajů, a to jasným, snadno přístupným, stručným, transparentním a srozumitelným způsobem. Informace by měly zahrnovat účel zpracování, totožnost správce údajů, práva zpřístupněná správcí údajů a další informace, je-li to potřeba k zajištění korektnosti. Za jistých okolností mohou z tohoto práva existovat výjimky, například v zájmu zabezpečení vyšetřování trestných činů, národní bezpečnosti, nezávislosti soudnictví a soudních řízení nebo jiných důležitých cílů obecného veřejného zájmu, jak je uvedeno v článku 23 obecného nařízení o ochraně osobních údajů.

8) Právo na přístup, opravu, výmaz a námitku

Subjekt údajů by měl být oprávněn získat potvrzení o tom, zda probíhá, nebo neprobíhá zpracování údajů týkajících se jeho osoby, a také přístup ke svým údajům, včetně kopií všech údajů týkajících se jeho osoby, které se zpracovávají.

Subjekt údajů by měl mít právo na případnou opravu svých údajů ze stanovených důvodů, například ukáže-li se, že jsou nepřesné nebo neúplné, a na výmaz svých údajů, jestliže například zpracování již není nutné nebo je protiprávní.

Subjekt údajů by rovněž měl mít právo kdykoli vznést na základě závažných oprávněných důvodů vztahujících se k jeho konkrétní situaci námitku proti zpracování svých údajů, jsou-li splněny konkrétní podmínky stanovené v právním rámci třetí země. V případě obecného nařízení o ochraně osobních údajů zahrnují takové podmínky například zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu, zpracování nezbytné při výkonu veřejné moci, kterým je správce pověřen, či zpracování nezbytné pro uskutečnění oprávněných zájmů správce údajů nebo třetí strany.

Výkon těchto práv by pro subjekt údajů neměl být příliš těžkopádný. Možná omezení těchto práv mohou existovat například v zájmu zabezpečení vyšetřování trestných činů, národní bezpečnosti, nezávislosti soudnictví a soudních řízení nebo jiných důležitých cílů obecného veřejného zájmu, jak je uvedeno v článku 23 obecného nařízení o ochraně osobních údajů.

9) Omezení dalšího předávání

Další předávání osobních údajů, které provádí původní příjemce původně získaných údajů, by mělo být povoleno, pouze pokud i další příjemce (tj. příjemce dále předávaných údajů) je také podřízen pravidlům (včetně smluvních pravidel) zaručujícím odpovídající úroveň ochrany a postupuje-li podle příslušných pokynů, pakliže se údaje zpracovávají jménem správce. Úroveň ochrany fyzických osob, jejichž údaje se předávají, se dalším předáváním nesmí oslabovat. V případě neexistence rozhodnutí o odpovídající ochraně odpovídá za zajištění náležitých záruk při dalším předávání údajů původní příjemce údajů předávaných z EU. Taková další předávání by se měla uskutečňovat jen k omezeným a stanoveným účelům a existuje-li pro takové zpracování platný právní důvod.

B. Příklady dalších obsahových zásad uplatňovaných při konkrétních typech zpracování:

1) Zvláštní kategorie údajů

Zvláštní ochranná opatření je třeba přijmout v případech, kdy se zpracovávají „zvláštní kategorie údajů“¹². Tyto kategorie by měly odpovídat kategoriím uvedeným v člancích 9 a 10 obecného nařízení o ochraně osobních údajů. Tato ochrana by měla být zavedena prostřednictvím přísnějších požadavků na zpracování údajů, například nutnosti výslovného souhlasu subjektu údajů se zpracováním, nebo prostřednictvím dalších bezpečnostních opatření.

¹² V bodě odůvodnění 10 obecného nařízení o ochraně osobních údajů jsou tyto zvláštní kategorie nazývány také „citlivé osobní údaje“.

2) Přímý marketing

Zpracovávají-li se údaje pro účely přímého marketingu, měl by subjekt údajů mít možnost kdykoli bezplatně vznést námitku proti zpracování svých údajů pro tyto účely.

3) Automatizované rozhodování a profilování

Rozhodnutí vycházející výlučně z automatizovaného zpracování (automatizované individuální rozhodování), včetně profilování, která mají pro subjekt údajů právní účinky nebo se jej významně dotýkají, mohou probíhat jen za určitých podmínek stanovených v právním rámci třetí země. V Evropském rámci taková rozhodnutí zahrnují například nutnost získat výslovný souhlas subjektu údajů nebo nezbytnost takového rozhodnutí pro uzavření smlouvy. Jestliže rozhodnutí podle právního rámce třetí země takové podmínky nesplňují, měl by mít subjekt údajů právo nebýt jejich předmětem. Právo třetí země by v každém případě mělo zajišťovat nezbytné záruky, včetně práva být informován o konkrétních důvodech pro rozhodnutí a jeho logice, opravit nepřesné nebo neúplné informace a napadnout rozhodnutí přijaté na základě nesprávného skutkového stavu.

C. Procesní a donucovací mechanismy:

Ačkoli se prostředky, které třetí země využívá k zajištění odpovídající ochrany, mohou lišit od prostředků zavedených v rámci Evropské unie¹³, musí být v systému odpovídajícím evropskému systému přítomny následující prvky:

1) Příslušný nezávislý dozorový úřad

Ve třetí zemi by měl existovat aspoň jeden nezávislý dozorový úřad pověřený sledováním, zajišťováním a vymáháním souladu s ustanoveními o ochraně údajů a soukromí. Tento dozorový úřad musí při výkonu svých povinností a pravomocí jednat naprosto nezávisle a nestranně a nesmí při něm vyžadovat ani přijímat pokyny. V této souvislosti by dozorový úřad měl disponovat všemi nezbytnými a dostupnými pravomocemi a posláním k zajišťování souladu s právy na ochranu údajů a k podporování informovanosti. Rovněž by se měl zohlednit personál a rozpočet dozorového úřadu. Dozorový orgán musí být také schopen provádět vyšetřování z vlastního podnětu.

2) Systém na ochranu údajů musí zajišťovat dobrou úroveň dodržování předpisů

Systém třetí země by měl zajistit vysokou míru odpovědnosti a informovanosti, a to jak u správců a subjektů zpracovávajících osobní údaje jejich jménem v oblasti jejich povinností, úkolů a odpovědností, tak u subjektů údajů v oblasti jejich práv a prostředků k výkonu těchto práv. Významnou roli v zajišťování dodržování předpisů může hrát existence účinných a odrazujících sankcí a samozřejmě také systémy přímého ověřování uskutečňované orgány, auditory či nezávislými osobami pověřenými ochranou údajů.

3) Odpovědnost

Rámec třetí země pro ochranu údajů by měl správcům údajů a subjektům zpracovávajícím osobní údaje jejich jménem ukládat povinnost dodržovat je a prokazovat jeho dodržování, a to především před příslušným dozorovým úřadem. Taková opatření mohou zahrnovat například posuzování vlivu na ochranu osobních údajů, vedení záznamů a protokolů o činnostech v oblasti zpracování údajů po stanovenou dobu, jmenování pověřence pro ochranu osobních údajů a záměrnou a standardní ochranu osobních údajů.

¹³ Věc C-362/14, Maximilian Schrems proti Data Protection Commissioner, 6. října 2015, odstavec 74.

4) Systém na ochranu údajů musí jednotlivým subjektům údajů při výkonu jejich práv poskytovat podporu a pomoc a příslušné mechanismy nápravy

Osoby musí mít možnost uplatnit opravné prostředky, aby rychle, účinně a bez nepřiměřených nákladů prosadily svá práva a zároveň zajistily dodržování předpisů. Za tímto účelem musí být zavedeny mechanismy dozoru, které v praxi umožňují nezávisle vyšetřovat stížnosti a odhalovat a postihovat případy porušení práva na ochranu údajů a práva na respektování soukromého života.

V případě nedodržení předpisů by subjekt údajů měl mít k dispozici účinné správní a soudní opravné prostředky, včetně náhrady škod vzniklých následkem protiprávního zpracování jeho osobních údajů. Jedná se o klíčový prvek, který musí zahrnovat systém nezávislé rozhodčí nebo soudní služby umožňující v příslušných případech vyplacení náhrad a uložených sankcí.

Kapitola 4: Základní záruky přístupu pro účely prosazování práva a národní bezpečnosti ve třetích zemích, kterými se omezuje zásah do základních práv

Při posuzování odpovídající úrovně ochrany podle ustanovení čl. 45 odst. 2 písm. a) se vyžaduje, aby Komise vzala v úvahu „*příslušné právní předpisy, obecné i odvětvové, včetně těch, které se týkají veřejné bezpečnosti, obrany, národní bezpečnosti a trestního práva a přístupu orgánů veřejné moci k osobním údajům, jakož i provádění těchto právních předpisů...*“.

Soudní dvůr ve věci Schrems podotýká, že „výraz ‚odpovídající úroveň ochrany‘ [...] musí být chápán v tom smyslu, že vyžaduje, aby tato třetí země skutečně zajišťovala na základě svých vnitrostátních předpisů nebo svých mezinárodních závazků takovou úroveň ochrany základních práv a svobod, jaká je rovnocenná úrovni zaručené v rámci Unie na základě směrnice 95/46 vykládané ve světle Listiny“. Ačkoli prostředky, které třetí země v této souvislosti využívá, se mohou lišit od prostředků zavedených v rámci Evropské unie, musí se tyto prostředky v praxi jevit jako účinné¹⁴.

V této souvislosti Soudní dvůr rovněž kriticky připomněl, že rozhodnutí podle zásady bezpečného přístavu „*neobsahuje žádné zjištění ohledně existence pravidel státního charakteru ve Spojených státech, jež mají omezit případné zásahy do základních práv osob, jejichž osobní údaje jsou předávány z Unie do Spojených států, tj. zásahy, jež by státní subjekty této země byly oprávněny činit v případě, že sledují takové legitimní cíle, jako je bezpečnost státu*“.

Skupina WP29 přijala dne 13. dubna 2016 v pracovním dokumentu WP237 základní záruky, které zohledňují judikaturu Soudního dvora a Evropského soudu pro lidská práva v oblasti dozoru. Ačkoli podrobná doporučení uvedená v dokumentu WP237 zůstávají v platnosti a mělo by se k nim přihlídnout při posuzování odpovídající úrovně třetí země v oblasti dozoru, uplatňování těchto záruk v oblasti prosazování práva a přístupu k údajům pro účely národní bezpečnosti se může lišit. Má-li se však ochrana považovat za odpovídající, je třeba, aby všechny třetí země při přístupu k údajům, ať už pro účely národní bezpečnosti nebo prosazování práva, dodržovaly tyto čtyři záruky:

- 1) Zpracování musí probíhat dle jasných, přesných a přístupných předpisů (právní základ).**
- 2) Je nutné prokázat jeho potřebnost a přiměřenost ve vztahu ke sledovaným legitimním cílům.**
- 3) Nad zpracováním musí probíhat nezávislý dohled.**
- 4) Osobám musí být k dispozici účinná právní ochrana.**

¹⁴ Věc C-362/14, Maximilian Schrems proti Data Protection Commissioner, 6. října 2015, odstavec 74.