



18/SK

WP 254 rev.01

| |
|--|
| Pracovná skupina zriadená podľa článku 29 |
|--|

Referenčné kritérium primeranosti

Prijaté 28. novembra 2017

naposledy revidované a prijaté 6. februára 2018

Táto pracovná skupina bola zriadená podľa článku 29 smernice 95/46/ES. Je nezávislým európskym poradným orgánom pre ochranu údajov a súkromia. Jej úlohy sú definované v článku 30 smernice 95/46/ES a článku 15 smernice 2002/58/ES.

Úlohy sekretariátu poskytuje riaditeľstvo C (základné práva a občianstvo Únie) Európskej komisie, generálne riaditeľstvo pre spravodlivosť, B-1049 Brusel, Belgicko, úrad č. MO-59 02/013.

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

Úvod

Pracovná skupina orgánov EÚ na ochranu osobných údajov¹ (pracovná skupina podľa článku 29) v minulosti vypracovala pracovný dokument o prenosoch údajov do tretích krajín (WP12)². V súvislosti s nahradením smernice všeobecným nariadením EÚ o ochrane údajov (GDPR)³, pracovná skupina podľa článku 29 reviduje pracovný dokument WP12, teda svoje skoršie usmernenie, s cieľom aktualizovať ho v kontexte nových právnych predpisov a nedávnej judikatúry Súdneho dvora⁴.

Cieľom tohto pracovného dokumentu je aktualizovať Prvú kapitolu pracovného dokumentu WP12 týkajúcu sa ústrednej otázky primeranej úrovne ochrany údajov v tretej krajine, na území alebo v jednom či viacerých určených sektoroch v danej tretej krajine alebo predmetnej medzinárodnej organizácii (ďalej len: „tretie krajiny alebo medzinárodné organizácie“). Tento dokument bude priebežne revidovaný a v prípade potreby v budúcnosti aktualizovaný, a to na základe praktických skúseností získaných prostredníctvom uplatňovania GDPR. Kapitola 2 (*Uplatňovanie prístupu na krajiny, ktoré ratifikovali Dohovor 108*) a kapitola 3 (*Uplatňovanie prístupu na odvetvovú samoreguláciu*) dokumentu WP12 by sa mali aktualizovať neskôr.

Tento pracovný dokument sa zameriava výlučne na rozhodnutia o primeranosti, ktoré sú vykonávacími aktmi⁵ Európskej komisie, podľa článku 45 GDPR. Ďalšie aspekty prenosov osobných údajov do tretích krajín a medzinárodných organizácií budú preskúmané v nasledujúcich pracovných dokumentoch, ktoré budú zverejnené samostatne (záväzné vnútropodnikové pravidlá, výnimky).

Cieľom tohto dokumentu je poskytnúť usmernenia Európskej komisii a pracovnej skupine podľa článku 29 podľa GDPR k posudzovaniu úrovne ochrany údajov v tretích krajinách a medzinárodných organizáciách, a to stanovením základných zásad ochrany údajov, ktoré sa musia nachádzať v právnom rámci tretej krajiny alebo medzinárodnej organizácie s cieľom zabezpečiť zásadnú rovnocennosť s rámcom EÚ. Okrem toho môže tento dokument usmerniť tretie krajiny a medzinárodné organizácie, ktoré majú záujem získať primeranosť. Zásady stanovené v tomto pracovnom dokumente však nie sú určené priamo prevádzkovateľom alebo sprostredkovateľom údajov.

Tento dokument pozostáva zo štyroch kapitol:

Kapitola 1: niektoré všeobecné informácie týkajúce sa koncepcie primeranosti

Kapitola 2: procesné aspekty záverov o primeranosti podľa GDPR

Kapitola 3: všeobecné zásady ochrany údajov. Táto kapitola obsahuje základné všeobecné zásady ochrany údajov s cieľom zabezpečiť, aby úroveň ochrany údajov v tretej krajine alebo medzinárodnej organizácii bola v podstate rovnocenná s úrovňou ochrany stanovenou právnymi predpismi EÚ.

Kapitola 4: Základné záruky v oblasti presadzovania práva a prístupu na účely národnej bezpečnosti na obmedzenie zásahov do základných práv. Táto kapitola obsahuje základné záruky v oblasti presadzovania práva a prístupu na účely národnej bezpečnosti v nadväznosti na rozsudok Súdneho dvora z roku 2015 a na základe pracovného dokumentu pracovnej skupiny podľa článku 29 o základných zárukách, prijatého v roku 2016.

¹ Ako sa stanovuje v článku 29 smernice EÚ o ochrane osobných údajov 95/46/ES.

² WP12, „Pracovný dokument: prenosy osobných údajov do tretích krajín: uplatňovanie článkov 25 a 26 smernice EÚ o ochrane osobných údajov“ prijatý pracovnou skupinou 24. júla 1998.

³ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Text s významom pre EHP).

⁴ Vrátane veci C-362/14, Maximillian Schrems/komisár pre ochranu údajov, 6. októbra 2015.

⁵ Pozri príslušný článok 45 ods. 3 a článok 93 ods. 2 GDPR, pokiaľ ide o ďalšie informácie o vykonávacích aktoch.

Kapitola 1: niektoré všeobecné informácie týkajúce sa koncepcie primeranosti

V článku 45 ods. 1 GDPR sa stanovuje zásada, že prenosy údajov do tretej krajiny alebo medzinárodnej organizácie sa uskutočnia iba vtedy, ak tretia krajina, územie alebo jeden či viaceré určené sektory v danej tretej krajine alebo predmetná medzinárodná organizácia zaručujú primeranú úroveň ochrany.

Koncepcia „primeranej úrovne ochrany“, ktorá už existovala v rámci smernice 95/46/ES, bola ďalej rozvinutá Súdnym dvorom. V tomto bode je dôležité pripomenúť normu stanovenú Súdnym dvorom v rozsudku Schrems, a to že zatiaľ čo „úroveň ochrany“ v tretej krajine musí byť „v podstate rovnocenná“ úrovni ochrany zaručenej v EÚ, „prostriedky, ktoré v tomto ohľade použije táto tretia krajina na zabezpečenie takejto úrovne ochrany, môžu byť rozdielne od tých, ktoré sa zaviedli v rámci [EÚ]“⁶. Cieľom preto nie je odzrkadľovať každý jeden bod európskych právnych predpisov, ale stanoviť základné prvky – hlavné požiadavky týchto právnych predpisov.

Cieľom rozhodnutí o primeranosti zo strany Európskej komisie je formálne potvrdiť so záväznými účinkami na členské štáty⁷, že úroveň ochrany údajov v tretej krajine alebo v medzinárodnej organizácii je v podstate rovnocenná s úrovňou ochrany údajov v Európskej únii⁸. Primeranosť možno dosiahnuť kombináciou práv dotknutých osôb a povinností tých, ktorí spracúvajú údaje alebo ktorí vykonávajú kontrolu nad takýmto spracúvaním a dohľadom zo strany nezávislých orgánov. Pravidlá ochrany údajov sú však účinné len vtedy, ak sú vymožiteľné a v praxi sa dodržiavajú. Preto je potrebné zvážiť nielen obsah pravidiel týkajúcich sa osobných údajov prenášaných do tretej krajiny alebo medzinárodnej organizácie, ale aj systém zavedený na zabezpečenie účinnosti takýchto pravidiel. Účinné mechanizmy presadzovania sú mimoriadne dôležité pre účinnosť pravidiel ochrany údajov.

V článku 45 ods. 2 GDPR sa stanovujú prvky, ktoré Európska komisia zohľadňuje pri posudzovaní primeranosti úrovne ochrany v tretej krajine alebo medzinárodnej organizácii.

Komisia zohľadní napríklad právny štát, dodržiavanie ľudských práv a základných slobôd, príslušné právne predpisy, existenciu a účinné pôsobenie jedného či viacerých nezávislých dozorných orgánov a medzinárodné záväzky, ktoré tretia krajina alebo medzinárodná organizácia prevzala.

Preto je jasné, že každá zmysluplná analýza primeranej ochrany musí pozostávať z dvoch základných prvkov: z obsahu platných pravidiel a z prostriedkov na zabezpečenie ich účinného uplatňovania. Je na Európskej komisii, aby pravidelne overovala, či sú zavedené pravidlá v praxi účinné.

„Základ“ ochrany údajov, zásady „obsahu“ a „procesné požiadavky/požiadavky týkajúce sa presadzovania“, ktoré by sa mohli považovať za minimálnu požiadavku primeranej ochrany, vyplývajú z Charty základných práv EÚ a z GDPR. Okrem toho by sa mali zvážiť aj ďalšie medzinárodné dohody o ochrane údajov, napríklad Dohovor 108⁹.

Pozornosť sa musí venovať aj právnejmu rámcu pre prístup orgánov verejnej moci k osobným údajom. Ďalšie usmernenia v tejto súvislosti sa nachádzajú v pracovnom dokumente 237 (t. j. v dokumente o základných zárukách)¹⁰ o zárukách v kontexte dohľadu.

Všeobecné ustanovenia týkajúce sa ochrany údajov a súkromia v tretej krajine nie sú dostatočné. Naopak, do právneho rámca tretej krajiny alebo medzinárodnej organizácie sa musia zahrnúť osobitné ustanovenia týkajúce sa konkrétnych potrieb prakticky relevantných aspektov práva na ochranu údajov. Tieto ustanovenia musia byť vymožiteľné.

⁶ Vec C-362/14, Maximilian Schrems/komisár pre ochranu údajov, 6. októbra 2015 (body 73, 74).

⁷ Článok 288 ods. 2 ZFEÚ.

⁸ Vec C-362/14, Maximilian Schrems/komisár pre ochranu údajov, 6. októbra 2015 (bod 52).

⁹ Odôvodnenie 105 GDPR.

¹⁰ Pracovný dokument 01/2016 o odôvodnení zásahov do základných práv na súkromie a ochranu osobných údajov prostredníctvom opatrení dohľadu pri prenose osobných údajov (Európske základné záruky), 16/EN WP 237, 13. apríla 2016.

Kapitola 2: Procesné aspekty záverov o primeranosti podľa GDPR

Aby Európsky výbor pre ochranu údajov plnil svoju úlohu pri poskytovaní poradenstva Európskej komisii podľa článku 70 ods. 1 písm. s) GDPR, mala by sa Európskemu výboru pre ochranu údajov poskytnúť príslušná dokumentácia vrátane príslušnej korešpondencie a zistení Európskej komisie. Ak je právny rámec zložitý, malo by to zahŕňať každú vypracovanú správu o úrovni ochrany údajov tretej krajiny alebo medzinárodnej organizácie. V každom prípade by informácie poskytnuté Európskou komisiou mali byť úplné a Európsky výbor pre ochranu údajov by mal mať možnosť vykonať vlastné posúdenie týkajúce sa úrovne ochrany údajov v tretej krajine. Európsky výbor pre ochranu údajov včas vydá stanovisko k zisteniam Európskej komisie a určí nedostatky v rámci primeranosti, ak existujú. Európsky výbor pre ochranu údajov sa okrem toho bude snažiť navrhnúť zmeny alebo doplnenia na riešenie prípadných nedostatkov.

Podľa článku 45 ods. 4 GDPR je na Európskej komisii, aby priebežne monitorovala vývoj, ktorý by mohol ovplyvniť pôsobenie rozhodnutia o primeranosti.

V článku 45 ods. 3 GDPR sa stanovuje, že pravidelné preskúmanie sa musí uskutočniť najmenej raz za štyri roky. To je však všeobecný časový rámec, ktorý sa musí prispôbiť každej tretej krajine alebo medzinárodnej organizácii, v súvislosti s ktorou bolo vydané rozhodnutie o primeranosti. V závislosti od konkrétnych okolností by mohol byť opodstatnený aj kratší cyklus preskúmania. Okrem toho by k potrebe preskúmania skôr ako v pravidelnom čase mohli viesť incidenty alebo iné informácie o právnom rámci alebo zmeny v právnom rámci v príslušnej tretej krajine alebo medzinárodnej organizácii. Navyše sa zdá vhodné uskutočniť prvé preskúmanie úplne nového rozhodnutia o primeranosti skôr, a postupne upraviť cyklus preskúmania v závislosti od jeho výsledku.

Vzhľadom na úlohu poskytnúť Európskej komisii stanovisko k tomu, či tretia krajina, územie alebo jeden či viaceré určené sektory v tretej krajine alebo medzinárodná organizácia už nezaručujú primeranú úroveň ochrany, Európsky výbor pre ochranu údajov musí včas získať zmysluplné informácie týkajúce sa monitorovania príslušného vývoja v tejto tretej krajine alebo medzinárodnej organizácii zo strany Európskej komisie. Európsky výbor pre ochranu údajov by preto mal byť priebežne informovaný o každom procese preskúmania a hodnotiacej misii v tretej krajine alebo v medzinárodnej organizácii. Európsky výbor pre ochranu údajov by ocenil, keby bol vyzvaný, aby sa zúčastnil na týchto procesoch preskúmania a hodnotiacich misiách.

Okrem toho treba poznamenať, že podľa článku 45 ods. 5 GDPR má Európska komisia právo zrušiť, zmeniť alebo pozastaviť existujúce rozhodnutia o primeranosti. Do postupu zrušenia, zmeny alebo pozastavenia by mal následne byť zapojený Európsky výbor pre ochranu údajov, a to tak, že bude požiadaný o stanovisko podľa článku 70 ods. 1 písm. s).

Navyše, ako sa už uznáva v článku 58 ods. 5 GDPR a podľa rozhodnutia Súdneho dvora vo veci Schrems, orgány na ochranu údajov musia byť schopné sa obrátiť na súd, ak uznajú, že nárok osoby voči rozhodnutiu o primeranosti je oprávnený: „V tomto ohľade je úlohou vnútroštátneho zákonodarcu stanoviť prostriedky nápravy umožňujúce dotknutému vnútroštátnemu dozornému orgánu uplatniť výhrady, ktoré považuje za dôvodné, na vnútroštátnych súdoch, aby tieto podali, ak majú rovnaké pochybnosti ako tento orgán, pokiaľ ide o platnosť rozhodnutia Komisie, návrh na začatie prejudiciálneho konania na účely preskúmania platnosti tohto rozhodnutia“¹¹.

Kapitola 3: Všeobecné zásady ochrany údajov s cieľom zabezpečiť, aby úroveň ochrany v tretej krajine, na území alebo v jednom či viacerých určených sektoroch v danej tretej krajine alebo v medzinárodnej organizácii bola v podstate rovnocenná s úrovňou ochrany stanovenou právnymi predpismi EÚ

Systém tretej krajiny alebo medzinárodnej organizácie musí obsahovať tieto základné zásady a mechanizmy obsahu a procesné zásady a mechanizmy/zásady a mechanizmy presadzovania v súvislosti s ochranou údajov:

A. Zásady obsahu:

1. Pojmy

Mali by existovať základné pojmy a/alebo zásady v oblasti ochrany údajov. Tieto nemusia odzrkadľovať terminológiu GDPR, ale mali by odrážať pojmy zakotvené v európskych právnych predpisoch o ochrane údajov a mali by s nimi byť v súlade. GDPR napríklad obsahuje tieto dôležité pojmy: „osobné údaje“, „spracúvanie osobných údajov“, „prevádzkovateľ“, „sprostredkovateľ“, „príjemca“, „citlivé údaje“.

2. Dôvody zákonného a spravodlivého spracúvania na legítimne účely

Údaje sa musia spracúvať zákonným, spravodlivým a legítimným spôsobom.

Legitímne základy, podľa ktorých možno osobné údaje zákonne, spravodlivo a oprávnene spracúvať, by sa mali stanoviť dostatočne jasným spôsobom. V európskom rámci sa uznáva niekoľko takýchto legítimných dôvodov, ako sú napríklad ustanovenia vo vnútroštátnych právnych predpisoch, súhlas dotknutej osoby, plnenie zmluvy alebo oprávnený záujem prevádzkovateľa alebo tretej strany, ktorý neprevažuje nad záujmami jednotlivca.

3. Zásada obmedzenia účelu

Údaje by sa mali spracúvať na konkrétny účel a následne by sa mali použiť len vtedy, keď to nie je nezlučiteľné s účelom spracúvania.

4. Zásada kvality údajov a zásada proporcionality

Údaje by mali byť presné a v prípade potreby udržiavané aktuálne. Údaje by mali byť primerané, relevantné a nie neúmerné vo vzťahu k účelom, na ktoré sa spracúvajú.

5. Zásada uchovávania údajov

Údaje by sa vo všeobecnosti nemali uchovávať dlhšie, než je potrebné na účely, na ktoré sa osobné údaje spracúvajú.

6. Zásada bezpečnosti a dôvernosti

Každý subjekt, ktorý spracúva osobné údaje, by mal zabezpečiť, aby sa údaje spracúvali spôsobom, ktorý zaručuje bezpečnosť osobných údajov vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení. Úroveň bezpečnosti by mala zohľadňovať najnovšie poznatky a súvisiace náklady.

7. Zásada transparentnosti

Každý jednotlivец by mal byť informovaný o všetkých hlavných prvkoch spracúvania jeho osobných údajov, a to jasným, ľahko dostupným, stručným, transparentným a zrozumiteľným spôsobom. Takéto informácie by mali zahŕňať účel spracúvania, totožnosť prevádzkovateľa, práva, ktoré má k dispozícii a iné informácie, pokiaľ je to nevyhnutné na zabezpečenie spravodlivosti. Za určitých podmienok môžu existovať niektoré výnimky z tohto práva na informácie, napríklad keď ide o ochranu trestného vyšetrovania, národnú bezpečnosť, nezávislosť súdov a súdne konania alebo iné dôležité ciele všeobecného verejného záujmu, ako je to v prípade článku 23 GDPR.

8. Právo na prístup, opravu, vymazanie a právo namietat'

Dotknutá osoba by mala mať právo získať potvrdenie o tom, či sa spracúvanie, ktoré sa jej týka, uskutočňuje alebo nie, ako aj prístup k svojim údajom vrátane získania kópie všetkých údajov súvisiacich s ňou, ktoré sa spracúvajú.

Dotknutá osoba by podľa potreby mala mať právo na opravu svojich údajov, a to z osobitných dôvodov, napríklad ak sa preukáže, že sú nesprávne alebo neúplné, ako aj na vymazanie svojich osobných údajov, ak napríklad ich spracúvanie už nie je nevyhnutné alebo je nezákonné.

Dotknutá osoba by okrem toho mala mať právo kedykoľvek na základe nevyhnutných oprávnených dôvodov týkajúcich sa jej konkrétnej situácie vzniesť námietku voči spracúvaniu jej údajov za osobitných podmienok stanovených v právnom rámci tretej krajiny. V GDPR takéto podmienky zahŕňajú napríklad situácie, keď je spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu alebo keď je potrebné na výkon verejnej moci zverenej prevádzkovateľovi, alebo keď je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana.

Výkon týchto práv by pre dotknutú osobu nemal byť príliš náročný. Môžu existovať prípadné výnimky z týchto práv, napríklad keď ide o ochranu trestného vyšetrovania, národnú bezpečnosť, nezávislosť súdov a súdne konania alebo iné dôležité ciele všeobecného verejného záujmu, ako je to v prípade článku 23 GDPR.

9. Obmedzenia následných prenosov

Ďalšie prenosy osobných údajov pôvodným príjemcom pôvodného prenosu údajov by sa mali povoliť len vtedy, keď ďalší príjemca (t. j. príjemca následného prenosu) takisto podlieha pravidlám (vrátane zmluvných pravidiel), pričom má primeranú úroveň ochrany a dodržiava príslušné pokyny pri spracúvaní údajov v mene prevádzkovateľa. Úroveň ochrany fyzických osôb, ktorých údaje sa prenášajú, nesmie byť narušená ďalším prenosom. Pôvodný príjemca údajov prenášaných z EÚ je povinný zabezpečiť, aby následné prenosy údajov poskytovali primerané záruky, ak neexistuje rozhodnutie o primeranosti. Takéto následné prenosy údajov by sa mali uskutočňovať len na obmedzené a určené účely a pokiaľ existuje právny základ na takéto spracúvanie.

B. Príklady ďalších obsahových zásad, ktoré sa majú uplatňovať na konkrétne typy spracúvania:

1. Osobitné kategórie údajov

Ak ide o osobitné kategórie údajov, mali by existovať osobitné záruky¹². Tieto kategórie by mali odzrkadľovať kategórie zakotvené v článkoch 9 a 10 GDPR. Táto ochrana by sa mala zaviesť prostredníctvom náročnejších požiadaviek na spracúvanie údajov, napríklad že dotknutá osoba dá svoj výslovný súhlas na spracúvanie alebo prostredníctvom dodatočných bezpečnostných opatrení.

¹²

Takéto osobitné kategórie sú známe aj ako „citlivé údaje“ v odôvodnení 10 GDPR.

2. Priamy marketing

Ak sa údaje spracúvajú na účely priameho marketingu, dotknutá osoba by mala mať kedykoľvek možnosť namietať proti spracúvaniu jej údajov na takéto účely, a to bezplatne.

3. Automatizované rozhodovanie a profilovanie

Rozhodnutia založené výlučne na automatizovanom spracúvaní (automatizované individuálne rozhodovanie) vrátane profilovania, ktoré majú právne účinky alebo významne ovplyvňujú dotknutú osobu, sa môžu uskutočniť iba za určitých podmienok stanovených v právnom poriadku tretej krajiny. V európskom rámci takéto podmienky zahŕňajú napríklad potrebu získať výslovný súhlas dotknutej osoby alebo nevyhnutnosť takéhoto rozhodnutia na účely uzatvorenia zmluvy. Ak rozhodnutie nie je v súlade s podmienkami stanovenými v právnom poriadku tretej krajiny, dotknutá osoba by mala mať právo nepodliehať mu. V právnom poriadku tretej krajiny by sa v každom prípade mali stanovovať potrebné záruky vrátane práva byť informovaný o konkrétnych dôvodoch, na ktorých sa zakladá rozhodnutie, a o príslušnom odôvodnení, práva na opravu nesprávnych a neúplných informácií, a práva napadnúť rozhodnutie, ak bolo prijaté na nesprávnom vecnom základe.

C. Procesné mechanizmy a mechanizmy presadzovania:

Hoci prostriedky, ktoré tretia krajina použije na zabezpečenie primeranej úrovne ochrany sa môžu líšiť od prostriedkov, ktoré sa používajú v rámci Európskej únie¹³, systém, ktorý je v súlade s európskym systémom sa musí vyznačovať prítomnosťou týchto prvkov:

1. Príslušný nezávislý dozorný orgán

V tretej krajine by mal existovať jeden alebo viac nezávislých dozorných orgánov, ktorých úlohou je monitorovanie, zabezpečovanie a presadzovanie dodržiavania ustanovení v oblasti ochrany údajov a súkromia. Dozorný orgán koná pri vykonávaní svojich povinností, pričom nesmie žiadať ani prijímať žiadne pokyny. V tejto súvislosti by dozorný orgán mal mať všetky potrebné a dostupné právomoci a úlohy, aby zabezpečil súlad s právami na ochranu údajov a podporoval informovanosť. Mal by sa zväžiť aj personál a rozpočet dozorného orgánu. Dozorný orgán by mal okrem toho mať možnosť uskutočňovať vyšetrovania na vlastný podnet.

2. Systém ochrany údajov musí zabezpečiť dobrú úroveň súladu

Systém tretej krajiny by mal zabezpečiť vysoký stupeň zodpovednosti a informovanosti medzi prevádzkovateľmi a tými, ktorí spracúvajú údaje v ich mene, o ich povinnostiach, úlohách a zodpovednostiach, a medzi dotknutými osobami o ich právach a o prostriedkoch ich vykonávania. Významnú úlohu v zabezpečení dodržiavania pravidiel môže zohrávať existencia účinných a odradzujúcich sankcií a samozrejme aj systémy priameho overenia orgánmi, audítormi alebo nezávislými úradníkmi na ochranu údajov.

3. Zodpovednosť

Rámcom ochrany údajov tretej krajiny by sa mala prevádzkovateľom a/alebo tým, ktorí spracúvajú osobné údaje v ich mene, uložiť povinnosť dodržiavať ho a vedieť preukázať takýto súlad najmä príslušnému dozornému orgánu. Takéto opatrenia môžu zahŕňať napríklad posúdenia vplyvu na ochranu údajov, vedenie záznamov alebo protokolových súborov o činnostiach spracúvania údajov počas primeraného obdobia, určenie úradníka pre ochranu údajov alebo špecificky navrhnuté a štandardnej ochrany údajov.

¹³

Vec C-362/14, Maximillian Schrems/komisár pre ochranu údajov, 6. októbra 2015, bod 74.

4. Systém ochrany údajov musí poskytovať podporu a pomoc jednotlivým dotknutým osobám pri výkone svojich práv a vhodné mechanizmy nápravy

Jednotlivec by mal mať možnosť uplatniť opravné prostriedky na rýchle a účinné presadzovanie svojich práv, a to bez príliš vysokých nákladov, ako aj na zabezpečenie súladu. Na to musia existovať mechanizmy dohľadu, ktoré umožňujú nezávislé vyšetrowanie sťažností a v praxi umožňujú identifikáciu a potrestanie každého porušenia práva na ochranu údajov a na rešpektovanie súkromného života.

Ak sa nedodržiavajú pravidlá, dotknutej osobe by sa mala poskytnúť aj účinná správna a súdna náprava vrátane náhrady škody v dôsledku nezákonného spracúvania jej osobných údajov. Toto je kľúčový prvok, ktorý musí zahŕňať systém nezávislého rozhodovania alebo arbitráže, ktorý umožňuje zaplatiť odškodnenie a podľa potreby uložiť sankcie.

Kapitola 4: základné záruky v tretích krajinách na obmedzenie zásahov do základných práv v prípade prístupu k údajom na účely presadzovania práva a na účely národnej bezpečnosti

Pri posudzovaní primeranosti úrovne ochrany je podľa článku 45 ods. 2 písm. a) Komisia povinná zohľadniť „príslušné právne predpisy, a to všeobecne aj odvetvové, vrátane predpisov týkajúcich sa verejnej bezpečnosti, obrany, národnej bezpečnosti a trestného práva a prístupu orgánov verejnej moci k osobným údajom, ako aj vykonávanie takýchto právnych predpisov...“.

Súdny dvor vo veci Schrems uviedol, že „výraz „primeraná úroveň ochrany“ však treba chápať v tom zmysle, že vyžaduje, aby táto tretia krajina skutočne zaistila z dôvodu jej vnútroštátneho práva alebo medzinárodných dohôd, ktoré podpísala, úroveň ochrany slobôd a základných práv, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie podľa smernice 95/46 v spojení s Chartou“. Aj keď prostriedky, ktoré v tomto ohľade využíva táto tretia krajina, môžu byť rozdielne od tých, ktoré sa využívajú v rámci Európskej únie, tieto prostriedky musia byť v praxi efektívne¹⁴.

V tomto kontexte súd kriticky pripomenul aj to, že predchádzajúce rozhodnutie bezpečného prístavu „neobsahuje nijaké ustanovenie, čo sa týka existencie pravidiel štátnej povahy v Spojených štátoch, ktorých cieľom by bolo obmedzenie prípadných zásahov do základných práv osôb, ktorých údaje sú prenesené z Únie do Spojených štátov, teda zásady, ktoré by subjekty verejnej moci tejto krajiny boli oprávnené uskutočniť v rámci sledovania legitímnych cieľov, akým je napríklad národná bezpečnosť“.

Pracovná skupina podľa článku 29 určila v stanovisku WP237, prijatom 13. apríla 2016, základné záruky odzrkadľujúce judikatúru Súdneho dvora a EDLP v oblasti dohľadu. Zatiaľ čo odporúčania uvedené v stanovisku WP237 sú naďalej platné a mali by sa zohľadniť pri posudzovaní primeranosti tretej krajiny v oblasti dohľadu, uplatňovanie týchto záruk sa môže líšiť v oblastiach presadzovania práva a prístupu k údajom na účely národnej bezpečnosti. Napriek tomu musia byť tieto štyri záruky rešpektované, pokiaľ ide o prístup k údajom, či už na účely národnej bezpečnosti, alebo na účely presadzovania práva, všetkými tretími krajinami, aby boli považované za primerané:

- 1. Spracúvanie by malo byť založené na jasných, presných a dostupných pravidlách (právny základ)**
- 2. Je nutné preukázať nevyhnutnosť a proporcionalitu, pokiaľ ide o sledované legitímne ciele**
- 3. Spracúvanie musí podliehať nezávislému dohľadu**
- 4. Fyzické osoby musia mať k dispozícii účinné prostriedky nápravy**