Zbierka súdnych rozhodnutí

ROZSUDOK SÚDNEHO DVORA (veľká komora)

zo 16. júla 2020*

„Návrh na začatie prejudiciálneho konania – Ochrana fyzických osôb pri spracovaní osobných údajov – Charta základných práv Európskej únie – Články 7, 8 a 47 – Nariadenie (EÚ) 2016/679 – Článok 2 ods. 2 – Pôsobnosť – Prenosy osobných údajov do tretích krajín na obchodné účely – Článok 45 – Rozhodnutie Komisie o primeranosti – Článok 46 – Prenosy vyžadujúce primerané záruky – Článok 58 – Právomoci dozorných orgánov – Spracúvanie prenesených údajov orgánmi verejnej moci tretej krajiny na účely národnej bezpečnosti – Posúdenie primeranosti úrovne ochrany zabezpečenej v tretej krajine – Rozhodnutie 2010/87/EÚ – Štandardné doložky o ochrane údajov pre prenos osobných údajov do tretích krajín – Primerané záruky poskytnuté prevádzkovateľom – Platnosť – Vykonávacie rozhodnutie (EÚ) 2016/1250 – Primeranosť ochrany poskytovanej štítom na ochranu osobných údajov medzi Európskou úniou a Spojenými štátmi – Platnosť – Sťažnosť fyzickej osoby, ktorej osobné údaje boli prenesené z Európskej únie do Spojených štátov“

Vo veci C-311/18,

ktorej predmetom je návrh na začatie prejudiciálneho konania podľa článku 267 ZFEÚ, podaný rozhodnutím High Court (Vyšší súd, Írsko) zo 4. mája 2018 a doručený Súdnemu dvoru 9. mája 2018, ktorý súvisí s konaním:

Data Protection Commissioner

proti

Facebook Ireland Ltd,

Maximillianovi Schremsovi,

za účasti:

The United States of America

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

SÚDNY DVOR (veľká komora),

v zložení: predseda K. Lenaerts, podpredsedníčka R. Silva de Lapuerta, predsedovia komôr A. Arabadžiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, L. S. Rossi a I. Jarukaitis, sudcovia M. Ilešič, T. von Danwitz (spravodajca) a D. Šváby,

* Jazyk konania: angličtina.

generálny advokát: H. Saugmandsgaard Øe,

tajomník: C. Strömholm, referentka,

so zreteľom na písomnú časť konania a po pojednávaní z 9. júla 2019,

so zreteľom na pripomienky, ktoré predložili:

– Data Protection Commissioner, v zastúpení: D. Young, solicitor, B. Murray a M. Collins, SC, a C. Donnelly, BL,

– Facebook Ireland Ltd, v zastúpení: P. Gallagher a N. Hyland, SC, A. Mulligan, a F. Kieran, BL, P. Nolan, C. Monaghan, C. O'Neill a R. Woulfe, solicitors,

– M. Schrems, v zastúpení: H. Hofmann, Rechtsanwalt, E. McCullough, SC, J. Doherty a S. O'Sullivan, SC, a G. Rudden, solicitor,

– The United States of America, v zastúpení: E. Barrington, SC, S. Kingston, BL, S. Barton a B. Walsh, solicitors,

– Electronic Privacy Information Centre, v zastúpení: S. Lucey, solicitor, G. Gilmore a A. Butler, BL, a C. O'Dwyer, SC,

– BSA Business Software Alliance Inc., v zastúpení: B. Van Vooren a K. Van Quathem, advocaten,

– Digitaleurope, v zastúpení: N. Cahill, barrister, J. Cahir, solicitor, a M. Cush, SC,

– Írsko, v zastúpení: A. Joyce a M. Browne, splnomocnení zástupcovia, za právnej pomoci D. Fennelly, BL,

– belgická vláda, v zastúpení: J.-C. Halleux a P. Cottin, splnomocnení zástupcovia,

– česká vláda, v zastúpení: M. Smolek, J. Vláčil, O. Serdula a A. Kasalická, splnomocnení zástupcovia,

– nemecká vláda, v zastúpení: J. Möller, D. Klebs a T. Henze, splnomocnení zástupcovia,

– francúzska vláda, v zastúpení: A.-L. Desjonquères, splnomocnená zástupkyňa,

– holandská vláda, v zastúpení: C. S. Schillemans, M. K. Bulterman a M. Noort, splnomocnené zástupkyne,

– rakúska vláda, v zastúpení: J. Schmoll a G. Kunnert, splnomocnení zástupcovia,

– poľská vláda, v zastúpení: B. Majczyna, splnomocnený zástupca,

– portugalská vláda, v zastúpení: L. Inez Fernandes, A. Pimenta a C. Vieira Guerra, splnomocnení zástupcovia,

– vláda Spojeného kráľovstva, v zastúpení: S. Brandon, splnomocnený zástupca, za právnej pomoci J. Holmes, QC, a C. Knight, barrister,

– Európsky parlament, v zastúpení: M. J. Martínez Iglesias a A. Caiola, splnomocnení zástupcovia,

– Európska komisia, v zastúpení: D. Nardi, H. Krämer a H. Kranenborg, splnomocnení zástupcovia,

– Európsky výbor pre ochranu údajov (EDPB), v zastúpení: A. Jelinek a K. Behn, splnomocnení zástupcovia,

po vypočutí návrhov generálneho advokáta na pojednávaní 19. decembra 2019,

vyhlásil tento

Rozsudok

1 Návrh na začatie prejudiciálneho konania sa v zásade týka:

– výkladu článku 3 ods. 2 prvej zarážky, článkov 25 a 26, ako aj článku 28 ods. 3 smernice Európskeho parlamentu a Rady 95/46/[ES] z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 1995, s. 31; Mim. vyd. 13/015, s. 355) v spojení s článkom 4 ods. 2 ZEÚ a článkami 7, 8 a 47 Charty základných práv Európskej únie (ďalej len „Charta“),

– výkladu a platnosti rozhodnutia Komisie 2010/87/EÚ z 5. februára 2010 o štandardných zmluvných doložkách pre prenos osobných údajov spracovateľom usadeným v tretích krajinách podľa smernice 95/46 (Ú. v. EÚ L 39, 2010, s. 5), zmeneného vykonávacím rozhodnutím Komisie (EÚ) 2016/2297 zo 16. decembra 2016 (Ú. v. EÚ L 2016, 344, s. 100) (ďalej len „rozhodnutie 2010/87“), ako aj

– výkladu a platnosti vykonávacieho rozhodnutia Komisie (EÚ) 2016/1250 z 12. júla 2016 podľa smernice 95/46 o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA (Ú. v. EÚ L 207, 2016, s. 1, ďalej len „rozhodnutie ŠnOOÚ“).

2 Tento návrh bol podaný v rámci sporu medzi Data Protection Commissioner (komisár pre ochranu údajov, Írsko) (ďalej len „komisár“), ďalej spoločnosťou Facebook Ireland Ltd a napokon pánom Maximillianom Schremsom vo veci sťažnosti, ktorú podal pán Schrems, v súvislosti s prenosom jeho osobných údajov spoločnosťou Facebook Ireland spoločnosti Facebook Inc. v Spojených štátoch.

Právny rámec

Smernica 95/46

3 Článok 3 smernice 95/46, nazvaný „Rozsah“, v odseku 2 stanovuje:

„Táto smernica sa neuplatňuje na spracovanie osobných údajov:

– v priebehu činností, ktoré sú mimo rozsahu zákona spoločenstva, ako sú tie, ktoré sú uvedené v hlave V a VI Zmluvy o Európskej únii a v žiadnom prípade sa neuplatňujú na operácie spracovania týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane hospodárskej prosperity štátu, keď sa operácia spracovania týka záležitostí bezpečnosti štátu) a činností štátu v oblastiach trestného zákona,

…“

4 Článok 25 tejto smernice stanovoval:

„1. Členské štáty zabezpečia, aby sa prenos osobných údajov… do tretej krajiny mohol urobiť len, bez toho, aby boli dotknuté vnútroštátne ustanovenia prijaté v súlade s ostatnými ustanoveniami tejto smernice, [ak – *neoficiálny preklad*] príslušná tretia krajina zaistí adekvátnu úroveň ochrany.

2. Adekvátnosť úrovne ochrany, ktorú poskytuje tretia krajina sa hodnotí vzhľadom na všetky okolnosti týkajúce sa operácie prenosu údajov alebo komplexu operácií prenosu údajov;…

…

6. Komisia môže zistiť [konštatovať – *neoficiálny preklad*], podľa postupu uvedeného v článku 31 ods. 2, že tretia krajina zaisťuje adekvátnu úroveň ochrany v rámci znenia odseku 2 tohto článku, z dôvodu jej vnútroštátneho práva alebo medzinárodných dohôd, ktoré podpísala, najmä na základe záverov jednaní uvedených v odseku 5, na ochranu súkromného života a osobných práv a slobôd [slobôd a základných práv osôb – *neoficiálny preklad*].

Členské štáty prijmú opatrenia potrebné na dosiahnutie súladu s rozhodnutím Komisie.“

5 Článok 26 ods. 2 a 4 uvedenej smernice stanovoval:

„2. Bez toho, aby boli dotknuté ustanovenia odseku 1 môže členský štát schváliť prenos alebo súbor prenosov osobných údajov do tretej krajiny, ktorá nezaistí adekvátnu úroveň ochrany v rámci znenia článku 25 ods. 2, vtedy keď kontrolór uvádza záruky [prevádzkovateľ poskytuje dostatočné záruky – *neoficiálny preklad*] s ohľadom na ochranu súkromia a základných práv a slobôd jednotlivcov a pokiaľ ide o uplatnenie príslušných práv; takéto záruky môžu vyplývať najmä z príslušných zmluvných klauzúl.

…

4. Ak Komisia rozhodne, v súlade s postupom uvedenom v článku 31 ods. 2, že určité štandardné zmluvné klauzuly ponúkajú dostatočné záruky, ako sa to požaduje v odseku 2, členské štáty podniknú nevyhnutné opatrenia, na dosiahnutie súladu s rozhodnutím Komisie.“

6 V zmysle článku 28 ods. 3 tej istej smernice:

„Každý [Každý dozorný orgán – *neoficiálny preklad*] je zabezpečený [má – *neoficiálny preklad*] najmä:

– vyšetrovacími právomocami [vyšetrovacie právomoci – *neoficiálny preklad*], ako sú práva prístupu k údajom, tvoriacich záležitosť subjektu operácií spracovania [ktoré sú predmetom spracovania – *neoficiálny preklad*] a práva zbierať všetky nevyhnutné informácie pre plnenie jeho kontrolných povinností,

– efektívnymi právomocami intervencie [efektívne právomoci intervencie – *neoficiálny preklad*], ako sú napríklad doručenie stanovísk pred vykonaním operácii spracovania, podľa článku 20 a zabezpečenie príslušného zverejnenia takýchto stanovísk, nariadenie zablokovania, vymazania alebo zničenia údajov, uvalenie dočasného alebo úplného zákazu na spracovanie, upozornenie alebo pripomenutie kontrolórovi [prevádzkovateľovi – *neoficiálny preklad*], alebo oznámenie záležitosti vnútroštátnemu parlamentu alebo iným politickým inštitúciám,

– právomocou [právomoc – *neoficiálny preklad*] zaoberať sa právnymi postupmi tam, kde sa porušili vnútroštátne ustanovenia prijaté v súlade s touto smernicou alebo dať tieto porušenia do pozornosti súdnych orgánov.

…“

Nariadenie GDPR

7 Smernica 95/46 bola zrušená a nahradená nariadením 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 ruší smernica 95/46 (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 2016, s. 1, ďalej len „nariadenie GDPR“).

8 Odôvodnenia 6, 10, 101, 103, 104, 107 až 109, 114, 116 a 141 nariadenia GDPR stanovujú:

„(6) Rýchly technologický rozvoj a globalizácia so sebou priniesli nové výzvy v oblasti ochrany osobných údajov. Rozsah získavania a zdieľania a osobných údajov sa výrazne zväčšil. Technológia umožňuje súkromným spoločnostiam a orgánom verejnej moci pri výkone ich činností využívať osobné údaje v doteraz bezprecedentnom rozsahu. Fyzické osoby stále viac zverejňujú svoje osobné údaje, a to aj v globálnom meradle. Technológia transformovala hospodársky aj spoločenský život a mala by ďalej uľahčovať voľný tok osobných údajov v rámci Únie a prenos do tretích krajín a medzinárodným organizáciám a súčasne zaručiť vysokú úroveň ochrany osobných údajov.

…

(10) S cieľom zabezpečiť konzistentnú a vysokú úroveň ochrany fyzických osôb a odstrániť prekážky tokov osobných údajov v rámci Únie, úroveň ochrany práv a slobôd fyzických osôb pri spracúvaní týchto údajov by mala byť rovnaká vo všetkých členských štátoch. Konzistentné a jednotné uplatňovanie pravidiel ochrany základných práv a slobôd fyzických osôb pri spracúvaní osobných údajov by sa malo zabezpečiť v rámci celej Únie. Pokiaľ ide o spracúvanie osobných údajov na účely dodržania zákonnej povinnosti, plnenia úloh realizovaných vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, členské štáty by mali mať možnosť zachovať alebo zaviesť vnútroštátne predpisy, ktorými by sa spresnilo uplatňovanie pravidiel stanovených v tomto nariadení. Spolu so všeobecnými a horizontálnymi právnymi predpismi o ochrane údajov, ktorými sa vykonáva smernica 95/46/ES, prijali členské štáty viaceré sektorové právne predpisy v oblastiach, v ktorých sú potrebné špecifickejšie normy. Týmto nariadením sa tiež členským štátom dáva priestor na spresnenie svojich pravidiel vrátane pravidiel spracúvania osobitných kategórií osobných údajov (ďalej len ‚citlivé údaje‘). V danom rozsahu toto nariadenie nevylučuje právo členského štátu, ktorým sa vymedzujú okolnosti špecifických spracovateľských situácií vrátane presnejšieho stanovenia podmienok, za ktorých je spracúvanie osobných údajov v súlade so zákonom.

…

(101) Toky osobných údajov do krajín mimo Únie a medzinárodným organizáciám aj z takýchto krajín a medzinárodných organizácií sú potrebné pre rozmach medzinárodného obchodu a medzinárodnú spoluprácu. Zvyšovanie takýchto tokov so sebou prinieslo nové výzvy a potreby týkajúce sa ochrany osobných údajov. Úroveň ochrany údajov fyzických osôb zaručovaná Úniou na základe tohto nariadenia by nemala byť ohrozená ani vtedy, keď sú osobné údaje prenášané z Únie prevádzkovateľom, sprostredkovateľom alebo iným príjemcom v tretích krajinách alebo medzinárodným organizáciám, a to ani v prípadoch následného prenosu osobných údajov z tretej krajiny alebo medzinárodnej organizácie prevádzkovateľom, sprostredkovateľom v rovnakej alebo inej tretej krajine alebo medzinárodnej organizácii. V každom prípade sa prenosy do tretích krajín a medzinárodným organizáciám môžu vykonávať len v úplnom súlade s týmto nariadením. Prenos by sa mohol uskutočniť len vtedy, ak s výhradou ostatných ustanovení v tomto nariadení prevádzkovateľ alebo sprostredkovateľ splnili podmienky stanovené v tomto nariadení týkajúce sa prenosu osobných údajov do tretích krajín alebo medzinárodným organizáciám.

…

(103) Komisia môže s účinnosťou pre celú Úniu rozhodnúť, že tretia krajina, územie alebo určený sektor v tretej krajine alebo medzinárodná organizácia zaručuje primeranú úroveň ochrany údajov, čím zaisťuje právnu istotu a jednotnosť v celej Únii, pokiaľ ide o tretiu krajinu alebo medzinárodnú organizáciu, ktorá sa považuje za tretiu krajinu alebo medzinárodnú organizáciu poskytujúcu takúto úroveň ochrany. V takýchto prípadoch sa prenosy osobných údajov do tejto tretej krajiny alebo medzinárodnej organizácii môžu uskutočňovať bez potreby získania ďalšieho povolenia. Komisia môže tiež rozhodnúť takéto rozhodnutie odvolať po tom, ako to tretej krajine alebo medzinárodnej organizácii oznámi a v plnom rozsahu odôvodní.

(104) V súlade so základnými hodnotami, na ktorých je založená Únia, najmä pokiaľ ide o ochranu ľudských práv, by Komisia mala pri posúdení tretej krajiny alebo územia či určeného sektora v tretej krajine zohľadniť skutočnosť, ako príslušná tretia krajina dodržiava zásady právneho štátu, prístupu k spravodlivosti a medzinárodné normy a štandardy v oblasti ľudských práv, ako aj jej všeobecné a odvetvové právo vrátane právnych predpisov týkajúcich sa verejnej bezpečnosti, obrany a národnej bezpečnosti, ako aj verejného poriadku a trestného práva. Pri prijímaní rozhodnutia o primeranosti týkajúceho sa územia alebo určeného sektora v tretej krajine by sa mali zohľadniť jasné a objektívne kritériá, ako sú napríklad osobitné spracovateľské činnosti a rozsah pôsobnosti uplatniteľných právnych noriem a platných právnych predpisov v tretej krajine. Tretia krajina by mala poskytnúť záruky, ktorými sa zaistí primeraná úroveň ochrany, ktorá v zásade zodpovedá úrovni zabezpečenej v rámci Únie, najmä ak sa osobné údaje spracúvajú v jednom alebo vo viacerých určených sektoroch. Tretia krajina by predovšetkým mala zabezpečiť účinný a nezávislý dozor nad ochranou údajov, ako aj mechanizmy spolupráce s orgánmi členských štátov na ochranu údajov a dotknutým osobám by sa mali poskytnúť účinné a vymožiteľné práva a účinné správne a súdne prostriedky nápravy.

…

(107) Komisia môže dospieť k záveru, že tretia krajina, územie alebo určený sektor v tretej krajine, alebo medzinárodná organizácia už nezaručujú primeranú úroveň ochrany údajov. V dôsledku toho by sa mal prenos osobných údajov do tejto tretej krajiny alebo medzinárodnej organizácii zakázať, pokiaľ nie sú splnené požiadavky tohto nariadenia týkajúce sa prenosov na základe primeraných záruk, vrátane záväzných vnútropodnikových pravidiel a výnimiek pre osobitné situácie. V takomto prípade by sa mali stanoviť postupy na účely konzultácií medzi Komisiou a takýmito tretími krajinami alebo medzinárodnými organizáciami. Komisia by mala včas informovať tretiu krajinu alebo medzinárodnú organizáciu o dôvodoch a začať s ňou konzultácie s cieľom napraviť tento stav.

(108) Pri absencii rozhodnutia o primeranosti by prevádzkovateľ alebo sprostredkovateľ mali prijať opatrenia na kompenzáciu za nedostatočnú ochranu údajov v tretej krajine prostredníctvom primeraných záruk pre dotknutú osobu. Takéto primerané záruky môžu spočívať v uplatnení záväzných vnútropodnikových pravidiel, štandardných doložiek o ochrane údajov prijatých Komisiou, štandardných doložiek o ochrane údajov prijatých dozorným orgánom, alebo zmluvných doložiek povolených dozorným orgánom. Tieto záruky by mali zabezpečiť súlad s požiadavkami na ochranu údajov a právami dotknutých osôb primeranými spracúvaniu v rámci Únie vrátane dostupnosti vymáhateľných práv dotknutých osôb a účinných právnych prostriedkov nápravy vrátane účinných prostriedkov správnej a súdnej nápravy a možnosti domáhať sa náhrady škody v Únii alebo tretej krajine. Mali by sa týkať predovšetkým súladu so všeobecnými zásadami spracúvania osobných údajov a zásad špecificky navrhnutej a štandardnej ochrany údajov. …

(109) Možnosť pre prevádzkovateľa alebo sprostredkovateľa uplatniť štandardné doložky o ochrane údajov prijaté Komisiou alebo dozorným orgánom by prevádzkovateľom ani sprostredkovateľom nemali brániť v tom, aby zahrnuli štandardné doložky o ochrane údajov do širšej zmluvy, ako napríklad zmluvy medzi sprostredkovateľom a ďalším sprostredkovateľom, alebo k nim pridali ďalšie doložky alebo dodatočné záruky, pokiaľ nie sú priamo alebo nepriamo v rozpore so štandardnými zmluvnými doložkami prijatými Komisiou alebo dozorným orgánom alebo pokiaľ sa nedotýkajú základných práv alebo slobôd dotknutých osôb. Prevádzkovatelia a sprostredkovatelia by sa mali nabádať, aby poskytovali dodatočné záruky prostredníctvom zmluvných záväzkov, ktoré doplnia štandardné ochranné doložky.

…

(114) V každom prípade, ak Komisia neprijala rozhodnutie o primeranej úrovni ochrany údajov v tretej krajine, prevádzkovateľ alebo sprostredkovateľ by mali využiť riešenia, ktoré dotknutým osobám poskytujú vymožiteľné a účinné práva, že budú aj naďalej môcť uplatňovať základné práva a záruky, pokiaľ ide o spracúvanie ich údajov v Únii, keď budú tieto údaje prenesené.

…

(116) Pri cezhraničnom pohybe osobných údajov mimo Úniu môže byť schopnosť fyzických osôb uplatniť si práva na ochranu údajov vystavená vyššiemu riziku, a to najmä pokiaľ ide o ich ochranu pred nezákonným využitím alebo poskytnutím týchto informácií. Zároveň môžu dozorné orgány zistiť, že nedokážu vybavovať sťažnosti alebo viesť vyšetrovania týkajúce sa činností vykonávaných za ich hranicami. Prekážkou v ich úsilí spolupracovať v cezhraničnom kontexte môžu byť aj nedostatočné preventívne alebo nápravné právomoci, nekonzistentné právne režimy a praktické prekážky, napríklad nedostatočné zdroje. …

…

(141) Každá dotknutá osoba by mala mať právo podať sťažnosť na jednom dozornom orgáne, a to predovšetkým v členskom štáte svojho obvyklého pobytu, a mať v súlade s článkom 47 Charty právo na účinný súdny prostriedok nápravy, ak sa domnieva, že boli porušené jej práva podľa tohto nariadenia, alebo ak dozorný orgán nereaguje na sťažnosť, čiastočne alebo v plnom rozsahu ju odmietne, nevyhovie jej alebo nekoná v prípade, keď je takéto konanie nevyhnutné na ochranu práv dotknutej osoby. …“

9 Článok 2 ods. 1 a 2 tohto nariadenia stanovuje:

„1. Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

2. Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov:

a) v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie;

b) členskými štátmi pri vykonávaní činností patriacich do rozsahu pôsobnosti kapitoly 2 hlavy V ZEÚ;

c) fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti;

d) príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania.“

10 Článok 4 tohto nariadenia stanovuje:

„Na účely tohto nariadenia:

…

2. ‚spracúvanie' je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami;

…

7. ‚prevádzkovateľ' je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu;

8. ‚sprostredkovateľ' je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa;

9. ‚príjemca' je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania;

…"

11 Článok 23 toho istého nariadenia stanovuje:

„1. V práve Únie alebo práve členského štátu, ktorému prevádzkovateľ alebo sprostredkovateľ podliehajú, sa prostredníctvom legislatívneho opatrenia môže obmedziť rozsah povinností a práv ustanovených v článkoch 12 až 22 a v článku 34, ako aj v článku 5, pokiaľ jeho ustanovenia zodpovedajú právam a povinnostiam ustanoveným v článkoch 12 až 22, ak takéto obmedzenie rešpektuje podstatu základných práv a slobôd a je nevyhnutným a primeraným opatrením v demokratickej spoločnosti s cieľom zaistiť:

a) národnú bezpečnosť;

b) obranu;

c) verejnú bezpečnosť;

d) predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie alebo výkon trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzanie;

…

2. Konkrétne musí každé legislatívne opatrenie uvedené v odseku 1 obsahovať osobitné ustanovenia, ktoré v relevantných prípado[ch] upravujú aspoň:

a) účely spracúvania alebo kategórie spracúvania;

b) kategórie osobných údajov;

c) rozsah zavedených obmedzení;

d) záruky zabraňujúce zneužitiu údajov alebo nezákonnému prístupu či prenosu;

e) určenie prevádzkovateľa alebo kategórií prevádzkovateľov;

f) doby uchovávania a uplatniteľné záruky, pričom sa zohľadní povaha, rozsah a účely spracúvania alebo kategórie spracúvania;

g) riziká pre práva a slobody dotknutých osôb a

h) práva dotknutých osôb na informovanie o obmedzení, pokiaľ tým nie je ohrozený účel obmedzenia.“

12 Kapitola V nariadenia GDPR, nazvaná „Prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám“, obsahuje články 44 až 50 tohto nariadenia. Podľa článku 44 tohto nariadenia s názvom „Všeobecná zásada prenosov“:

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

13 Článok 45 tohto nariadenia s názvom „Prenosy na základe rozhodnutia o primeranosti“ v odsekoch 1 až 3 stanovuje:

„1. Prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť, ak Komisia rozhodla, že tretia krajina, územie alebo jeden či viaceré určené sektory v danej tretej krajine alebo predmetná medzinárodná organizácia zaručujú primeranú úroveň ochrany. Na takýto prenos nie je nutné žiadne osobitné povolenie.

2. Pri posudzovaní primeranosti úrovne ochrany zohľadňuje Komisia najmä tieto skutočnosti:

a) právny štát, dodržiavanie ľudských práv a základných slobôd, príslušné právne predpisy, a to všeobecné 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, pravidiel ochrany údajov, profesijných pravidiel a bezpečnostných opatrení vrátane pravidiel pre následný prenos osobných údajov do ďalšej tretej krajiny alebo medzinárodnej organizácii, ktoré sa v danej tretej krajine alebo medzinárodnej organizácii dodržiavajú, judikatúr[u], ako aj účinné a vymáhateľné práva dotknutej osoby a účinné správne a súdne prostriedky nápravy pre dotknuté osoby, ktorých osobné údaje sa prenášajú;

b) existenci[u] a účinné pôsobenie jedného či viacerých nezávislých dozorných orgánov v predmetnej tretej krajine, alebo ktorému podlieha medzinárodná organizácia, so zodpovednosťou za zabezpečenie a presadzovanie dodržiavania pravidiel ochrany údajov vrátane primeraných právomocí pre presadzovanie práva, za poskytovanie pomoci a poradenstva dotknutým osobám pri výkone ich práv a za spoluprácu s dozornými orgánmi členských štátov; a

c) medzinárodné záväzky, ktoré dotknutá tretia krajina alebo medzinárodná organizácia prevzala, alebo iné záväzky vyplývajúce z právne záväzných dohovorov alebo nástrojov, ako aj z jej účasti na viacstranných alebo regionálnych systémoch, najmä vo vzťahu k ochrane osobných údajov.

3. Komisia môže po posúdení primeranosti úrovne ochrany rozhodnúť prostredníctvom vykonávacieho aktu, že tretia krajina, územie alebo jeden či viaceré určené sektory v tretej krajine alebo medzinárodná organizácia zaručujú primeranú úroveň ochrany v zmysle odseku 2 tohto článku. Vo vykonávacom akte sa stanoví mechanizmus pravidelného preskúmania, ktoré sa uskutočňuje najmenej raz za štyri roky, v ktorom sa zohľadnia všetky významné zmeny v tretej krajine alebo medzinárodnej organizácii. Vo vykonávacom akte sa uvedie rozsah jeho územnej a sektorovej pôsobnosti a v príslušných prípadoch aj dozorný orgán alebo dozorné orgány uvedené v odseku 2 písm. b) tohto článku. Vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 93 ods. 2“

14 Článok 46 daného nariadenia, nazvaný „Prenosy vyžadujúce primerané záruky“, v odsekoch 1 až 3 stanovuje:

„1. Ak neexistuje rozhodnutie podľa článku 45 ods. 3, prevádzkovateľ alebo sprostredkovateľ môže uskutočniť prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii len vtedy, ak prevádzkovateľ alebo sprostredkovateľ poskytol primerané záruky, a za podmienky, že dotknuté osoby majú k dispozícii vymožiteľné práva a účinné právne prostriedky nápravy.

2. Primerané záruky uvedené v odseku 1 sa môžu ustanoviť bez toho, aby sa dozorný orgán žiadal o akékoľvek osobitné povolenie, prostredníctvom:

a) právne záväzného a vykonateľného nástroja medzi orgánmi verejnej moci alebo verejnoprávnymi subjektmi;

b) záväzných vnútropodnikových pravidiel v súlade s článkom 47;

c) štandardných doložiek o ochrane údajov, ktoré prijala Komisia v súlade s postupom preskúmania uvedeným v článku 93 ods. 2;

d) štandardných doložiek o ochrane údajov, ktoré prijal dozorný orgán, a ktoré schválila Komisia podľa postupu preskúmania uvedeného v článku 93 ods. 2;

e) schváleného kódexu správania podľa článku 40 spolu so záväznými a vymáhateľnými záväzkami prevádzkovateľa alebo sprostredkovateľa v tretej krajine spočívajúcimi v uplatňovaní primeraných záruk, a to aj pokiaľ ide o práva dotknutých osôb, alebo

f) schváleného certifikačného mechanizmu podľa článku 42 spolu so záväzným a vymáhateľným záväzkom prevádzkovateľa alebo sprostredkovateľa v tretej krajine spočívajúcim v uplatňovaní primeraných záruk, a to aj pokiaľ ide o práva dotknutých osôb.

3. S výhradou povolenia od príslušného dozorného orgánu sa primerané záruky uvedené v odseku 1 môžu tiež zabezpečiť predovšetkým:

a) zmluvnými doložkami medzi prevádzkovateľom alebo sprostredkovateľom a prevádzkovateľom, sprostredkovateľom alebo príjemcom osobných údajov v tretej krajine alebo medzinárodnej organizácii, alebo

b) ustanoveniami, ktoré sa vložia do administratívnych dojednaní medzi orgánmi verejnej moci alebo verejnoprávnymi subjektmi a zahŕňajú vymožiteľné a účinné práva dotknutých osôb.“

15 Článok 49 toho istého nariadenia s názvom „Výnimky pre osobitné situácie“ stanovuje:

„1. Ak neexistuje rozhodnutie o primeranosti podľa článku 45 ods. 3 alebo ak neexistujú primerané záruky podľa článku 46 vrátane záväzných vnútropodnikových pravidiel, prenos alebo súbor prenosov osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa uskutoční len za jednej z týchto podmienok:

a) dotknutá osoba vyjadrila výslovný súhlas s navrhovaným prenosom po tom, ako bola informovaná o rizikách, ktoré takéto prenosy môžu pre ňu predstavovať z dôvodu absencie rozhodnutia o primeranosti a primeraných záruk;

b) prenos je nevyhnutný na plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom alebo na vykonanie predzmluvných opatrení prijatých na žiadosť dotknutej osoby;

c) prenos je nevyhnutný pre uzatvorenie alebo plnenie zmluvy uzatvorenej v záujme dotknutej osoby medzi prevádzkovateľom a inou fyzickou alebo právnickou osobou;

d) prenos je nevyhnutný z dôležitých dôvodov verejného záujmu;

e) prenos je nevyhnutný na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov;

f) prenos je nevyhnutný na ochranu životne dôležitých záujmov dotknutej osoby alebo iných osôb, ak je dotknutá osoba fyzicky alebo právne nespôsobilá vyjadriť súhlas;

g) prenos sa uskutočňuje z registra, ktorý je podľa práva Únie alebo práva členského štátu určený na poskytovanie informácií verejnosti a ktorý je otvorený na nahliadanie verejnosti alebo akejkoľvek osobe, ktorá vie preukázať oprávnený záujem, ale len pokiaľ sú v tomto konkrétnom prípade splnené podmienky stanovené právom Únie alebo právom členského štátu na nahliadanie.

Ak by sa prenos nemohol zakladať na ustanovení článku 45 alebo 46 vrátane ustanovení o záväzných vnútropodnikových pravidlách a neuplatňuje sa žiadna výnimka pre osobitnú situáciu uvedená v prvom pododseku tohto odseku, prenos do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť, len ak prenos nie je opakujúcej sa povahy, týka sa len obmedzeného počtu dotknutých osôb, je nevyhnutný na účely závažných oprávnených záujmov, ktoré sleduje prevádzkovateľ a nad ktorými neprevažujú záujmy alebo práva a slobody dotknutej osoby, a prevádzkovateľ posúdil všetky okolnosti sprevádzajúce prenos údajov a na základe tohto posúdenia poskytol vhodné záruky, pokiaľ ide o ochranu osobných údajov. Prevádzkovateľ informuje o prenose dozorný orgán. Prevádzkovateľ okrem poskytnutia informácií uvedených v článkoch 13 a 14 informuje dotknutú osobu o prenose a o závažných oprávnených záujmoch, ktoré sleduje.

2. Prenos podľa odseku 1 prvého pododseku písm. g) nezahŕňa všetky osobné údaje alebo celé kategórie osobných údajov obsiahnutých v registri. Ak je register určený na nahliadanie pre osoby s oprávneným záujmom, prenos sa uskutoční iba na žiadosť týchto osôb alebo vtedy, keď majú byť príjemcami.

3. Odsek 1 prvý pododsek písm. a), b) a c) a odsek 1 druhý pododsek sa neuplatňujú na činnosti, ktoré vykonávajú orgány verejnej moci pri uplatňovaní svojich verejných právomocí.

4. Verejný záujem uvedený v odseku 1 prvom pododseku písm. d) musí byť uznaný právom Únie alebo právom členského štátu, ktorému prevádzkovateľ podlieha.

5. Ak neexistuje rozhodnutie o primeranosti, môžu sa v práve Únie alebo v práve členského štátu zo závažných dôvodov verejného záujmu výslovne stanoviť obmedzenia prenosu osobitných kategórií osobných údajov do tretej krajiny alebo medzinárodnej organizácii. Členské štáty oznámia takéto ustanovenia Komisii.

6. Prevádzkovateľ alebo sprostredkovateľ zdokumentujú posúdenie, ako aj vhodné záruky uvedené v druhom pododseku odseku 1 tohto článku v záznamoch uvedených v článku 30.“

16 Podľa článku 51 ods. 1 nariadenia GDPR:

„Každý členský štát stanoví, že za monitorovanie uplatňovania tohto nariadenia je zodpovedný jeden alebo viacero nezávislých orgánov verejnej moci s cieľom chrániť základné práva a slobody fyzických osôb pri spracúvaní a uľahčiť voľný tok osobných údajov v rámci Únie (ďalej len ‚dozorný orgán‘).“

17 V súlade s článkom 55 ods. 1 tohto nariadenia „každý dozorný orgán je príslušný plniť úlohy, ktoré mu boli uložené, a vykonávať právomoci, ktoré mu boli zverené, v súlade s týmto nariadením na území vlastného členského štátu“.

18 Článok 57 ods. 1 uvedeného nariadenia stanovuje:

„Bez toho, aby boli dotknuté iné úlohy stanovené podľa tohto nariadenia, každý dozorný orgán na svojom území:

a) monitoruje a presadzuje uplatňovanie tohto nariadenia;

…

f) vybavuje sťažnosti podané dotknutou osobou alebo subjektom, organizáciou alebo združením v súlade s článkom 80, a vyšetruje v primeranom rozsahu podstatu sťažnosti a informuje sťažovateľa o pokroku a výsledkoch vyšetrovania v primeranej lehote, najmä ak je potrebné ďalšie vyšetrovanie alebo koordinácia s iným dozorným orgánom;

…“

19 V zmysle článku 58 ods. 2 a 4 toho istého nariadenia:

„2. Každý dozorný orgán má všetky tieto nápravné právomoci:

…

f) nariadiť dočasné alebo trvalé obmedzenie vrátane zákazu spracúvania;

…

j) nariadiť pozastavenie toku údajov príjemcovi v tretej krajine alebo medzinárodnej organizácii.

…

4. Výkon právomocí udelených dozornému orgánu podľa tohto článku podlieha primeraným zárukám vrátane účinného súdneho prostriedku nápravy a riadneho procesu, stanoveným v práve Únie a v práve členského štátu v súlade s chartou.“

20 Článok 64 ods. 2 nariadenia GDPR stanovuje:

„Ktorýkoľvek dozorný orgán, predseda [Európskeho výboru pre ochranu údajov (EDPB)] alebo Komisia môže požiadať, aby akúkoľvek záležitosť so všeobecným uplatnením alebo s účinkami vo viac ako jednom členskom štáte preskúmal výbor s cieľom získať stanovisko, najmä ak si príslušný dozorný orgán neplní povinnosti týkajúce sa vzájomnej pomoci podľa článku 61 alebo spoločných operácií podľa článku 62.“

21 Podľa článku 65 ods. 1 tohto nariadenia:

„S cieľom zabezpečiť správne a jednotné uplatňovanie tohto nariadenia v jednotlivých prípadoch prijme výbor záväzné rozhodnutie v týchto prípadoch:

…

c) ak príslušný dozorný orgán nepožiada výbor o stanovisko v prípadoch uvedených v článku 64 ods. 1 alebo nepostupuje podľa stanoviska výboru vydaného podľa článku 64. V tomto prípade môže záležitosť oznámiť výboru ktorýkoľvek dotknutý dozorný orgán alebo Komisia.“

22 Článok 77 uvedeného nariadenia, nazvaný „Právo na účinný súdny prostriedok nápravy voči rozhodnutiu dozorného orgánu“, stanovuje:

„1. Bez toho, aby boli dotknuté akékoľvek iné správne alebo súdne prostriedky nápravy, má každá dotknutá osoba právo podať sťažnosť dozornému orgánu, najmä v členskom štáte svojho obvyklého pobytu, mieste výkonu práce alebo v mieste údajného porušenia, ak sa domnieva, že spracúvanie osobných údajov, ktoré sa jej týka, je v rozpore s týmto nariadením.

2. Dozorný orgán, ktorému sa sťažnosť podala, informuje sťažovateľa o pokroku a výsledku sťažnosti vrátane možnosti podať súdny prostriedok nápravy podľa článku 78.“

23 Článok 78 toho istého nariadenia s názvom „Právo na účinný súdny prostriedok nápravy voči rozhodnutiu dozorného orgánu“ v odsekoch 1 a 2 stanovuje:

„1. Bez toho, aby boli dotknuté iné správne alebo mimosúdne prostriedky nápravy, každá fyzická alebo právnická osoba má právo na účinný súdny prostriedok nápravy voči právne záväznému rozhodnutiu dozorného orgánu, ktoré sa jej týka.

2. Bez toho, aby boli dotknuté iné správne alebo mimosúdne prostriedky nápravy, každá dotknutá osoba má právo na účinný súdny prostriedok nápravy, ak dozorný orgán, ktorý je príslušný podľa článkov 55 a 56, sťažnosť nevybavil alebo neinformoval dotknutú osobu do troch mesiacov o pokroku alebo výsledku sťažnosti podanej podľa článku 77.“

24 Článok 94 nariadenia GDPR stanovuje:

„1. Smernica [95/46] sa zrušuje s účinnosťou od 25. mája 2018.

2. Odkazy na zrušenú smernicu sa považujú za odkazy na toto nariadenie. Odkazy na Pracovnú skupinu pre ochranu jednotlivcov so zreteľom na spracovanie osobných údajov, zriadenú článkom 29 smernice [95/46], sa považujú za odkazy na Európsky výbor pre ochranu údajov zriadený týmto nariadením.“

25 Podľa článku 99 tohto nariadenia:

„1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

2. Uplatňuje sa od 25. mája 2018.“

Rozhodnutie 2010/87

26 Odôvodnenie 11 rozhodnutia 2010/87 znie:

„Dozorné orgány členských štátov hrajú kľúčovú úlohu v tomto zmluvnom mechanizme, pokiaľ ide o zabezpečenie primeranej ochrany osobných údajov po prenose. Vo výnimočných prípadoch, kedy vývozcovia údajov odmietnu alebo nie sú schopní poskytnúť dovozcovi údajov náležité pokyny, za bezprostredného rizika vážneho poškodenia subjektov údajov, majú štandardné zmluvné doložky umožniť dozorným orgánom audit dovozcov údajov a subdodávateľov spracovateľských operácií a v prípade potreby prijať rozhodnutia, ktoré sú pre dovozcov údajov a subdodávateľov záväzné. Dozorné orgány majú mať právomoc zakázať alebo pozastaviť prenos údajov alebo skupinu prenosov na základe štandardných zmluvných doložiek v tých výnimočných prípadoch, kde sa zistí, že prevod na zmluvnom základe bude mať pravdepodobne závažný nepriaznivý účinok na záruky a záväzky poskytujúce primeranú ochranu subjektu údajov.“

27 Článok 1 tohto rozhodnutia stanovuje:

„Štandardné zmluvné doložky uvedené v prílohe sa považujú za doložky, ktoré poskytujú primerané záruky, pokiaľ ide o ochranu súkromia a základných práv a slobôd jednotlivcov ako aj pokiaľ ide o uplatnenie príslušných práv, ako to požaduje článok 26 ods. 2 smernice [95/46].“

28 V súlade s článkom 2 druhým odsekom uvedeného rozhodnutia sa „toto rozhodnutie… bude týkať prenosu osobných údajov prevádzkovateľmi usadenými v Európskej únii príjemcom usadeným mimo územia Európskej únie, ktorí vykonávajú len funkciu spracovateľov“.

29 Článok 3 toho istého rozhodnutia stanovuje:

„Na účely tohto rozhodnutia sa uplatňujú tieto pojmy:

…

c) ‚vývozca údajov‘ je prevádzkovateľ, ktorý prenáša osobné údaje;

d) ‚dovozca údajov‘ je spracovateľ usadený v tretej krajine, ktorý súhlasí, že bude od vývozcu údajov prijímať osobné údaje určené na spracovanie v mene vývozcu údajov po prenose v súlade s jeho pokynmi a podmienkami tohto rozhodnutia a ktorý nepodlieha systému tretej krajiny zaisťujúcemu primeranú ochranu v zmysle článku 25 ods. 1 smernice [95/46];

…

f) ‚príslušné právo týkajúce sa ochrany údajov‘ sú právne predpisy chrániace základné práva a slobody jednotlivcov a najmä ich právo [právo na súkromie – *neoficiálny preklad*] vo vzťahu k spracovaniu osobných údajov, uplatniteľné na prevádzkovateľa údajov v členskom štáte, v ktorom je vývozca údajov usadený;

…“

30 Článok 4 rozhodnutia 2010/87 vo svojom pôvodnom znení, ktoré predchádzalo nadobudnutiu účinnosti vykonávacieho rozhodnutia 2016/2297, stanovoval:

„1. Bez toho, aby boli dotknuté ich právomoci podnikať právne opatrenia na zabezpečenie dodržiavania vnútroštátnych ustanovení prijatých podľa kapitol II, III, V a VI smernice [95/46], môžu príslušné úrady v členských štátoch uplatniť svoje existujúce právomoci zakázať alebo pozastaviť toky údajov do tretích krajín s cieľom ochrany osôb vo vzťahu k spracovaniu ich osobných údajov v prípadoch, ak:

a) sa zistí, že právo, ktorému vývozca údajov alebo subdodávateľ podlieha, mu ukladá povinnosti vo forme výnimky z príslušného práva týkajúceho sa ochrany údajov, ktoré presahujú obmedzenia nevyhnutné v demokratickej spoločnosti stanovené v článku 13 smernice [95/46], ak je pravdepodobné, že tieto povinnosti budú mať závažný nepriaznivý účinok na záruky poskytované príslušným právom týkajúcim sa ochrany údajov a štandardnými zmluvnými doložkami;

b) príslušný orgán zistí, že dovozca údajov alebo subdodávateľ nerešpektoval štandardné zmluvné doložky uvedené v prílohe, alebo

c) existuje veľká pravdepodobnosť, že štandardné zmluvné doložky uvedené v prílohe nie sú alebo nebudú dodržiavané a pokračujúcim prenosom by vzniklo bezprostredné riziko vážneho poškodenia subjektov údajov.

2. Zákaz alebo pozastavenie podľa odseku 1 bude zrušený, len čo dôvody pre pozastavenie alebo zákaz prestanú existovať.

3. Ak členské štáty prijmú opatrenia podľa odsekov 1 a 2, budú o tom bezodkladne informovať Komisiu, ktorá príslušné informácie postúpi ostatným členským štátom.“

31 Odôvodnenie 5 vykonávacieho rozhodnutia 2016/2297, ktoré bolo prijaté po vyhlásení rozsudku zo 6. októbra 2015, Schrems (C-362/14, EU:C:2015:650), znie takto:

„Rozhodnutie Komisie prijaté podľa článku 26 ods. 4 smernice [95/46] je *mutatis mutandis* záväzné pre všetky orgány členských štátov, ktoré sú jeho adresátmi, vrátane ich nezávislých orgánov dohľadu, v rozsahu, v akom má za následok, že uzná, že prenosy, ktoré sa uskutočňujú na základe štandardných zmluvných doložiek v ňom uvedených, ponúkajú dostatočné záruky, ako sa to požaduje v článku 26 ods. 2 príslušnej smernice. To nebráni vnútroštátnemu dozornému orgánu uplatňovať svoje právomoci pri dohľade nad tokmi údajov vrátane právomoci na pozastavenie alebo zákaz prenosu osobných údajov, keď skonštatuje, že sa prenos uskutočňuje v rozpore s právnymi predpismi EÚ a vnútroštátnymi právnymi predpismi o ochrane údajov, napríklad vtedy, keď príjemca údajov nedodržiava štandardné zmluvné doložky.“

32 Článok 4 rozhodnutia 2010/87 vo svojom aktuálnom znení, ktoré vychádza z vykonávacieho rozhodnutia 2016/2297, stanovuje:

„Keď príslušné orgány členských štátov uplatnia svoje právomoci podľa článku 28 ods. 3 smernice [95/46], dôsledkom čoho je pozastavenie alebo trvalý zákaz tokov údajov do tretích krajín v záujme ochrany fyzických osôb v súvislosti so spracovaním ich osobných údajov, príslušný členský štát o tom bezodkladne informuje Komisiu, ktorá príslušné informácie postúpi ostatným členským štátom.“

33 Príloha rozhodnutia 2010/87 s názvom „Štandardné zmluvné doložky (Spracovatelia)“ obsahuje 12 typových doložiek. Doložka 3 tejto prílohy, nazvaná „Doložka o oprávnenosti tretej strany“, stanovuje:

„1. Subjekt údajov môže ako oprávnená tretia strana uplatňovať voči vývozcovi údajov túto doložku, doložku 4 písm. b) až i), doložku 5 písm. a) až e) a písm. g) až j), doložku 6 ods. 1 a 2, doložku 7, doložku 8 ods. 2 a doložky 9 až 12.

2. Subjekt údajov môže uplatňovať voči dovozcovi údajov túto doložku, doložku 5 písm. a) až e) a písm. g), doložku 6, doložku 7, doložku 8 ods. 2 a doložky 9 až 12 v prípadoch, keď vývozca údajov fakticky zmizol alebo prestal právne existovať, pokiaľ prípadný nástupnícky subjekt neprevzal na základe zmluvy alebo podľa zákona všetky právne záväzky vývozcu údajov, v dôsledku čoho prijíma práva a záväzky vývozcu údajov a subjekt údajov ich v takom prípade môže uplatňovať voči tomuto subjektu.

…“

34 Z ustanovení doložky 4 tejto prílohy, nazvanej „Povinnosti vývozcu údajov“, vyplýva:

„Vývozca údajov súhlasí a zaručuje sa, že:

a) spracovanie osobných údajov vrátane ich prenosu bolo a bude aj naďalej vykonávané v súlade s relevantnými ustanoveniami príslušného práva týkajúceho sa ochrany údajov (a prípadne bolo oznámené príslušným orgánom členského štátu, v ktorom má vývozca údajov sídlo) a že neporušuje relevantné ustanovenia daného štátu;

b) nariadil a v priebehu trvania služieb spracovania osobných údajov bude nariaďovať dovozcovi údajov, aby prenášané osobné údaje spracovával len v mene vývozcu údajov a v súlade s príslušným právom týkajúcim sa ochrany osobných údajov a s doložkami;

…

f) ak bude prenos zahŕňať osobitné kategórie údajov, subjekt údajov bol alebo bude informovaný pred jeho uskutočnením alebo čo najskôr po ňom, že môže dôjsť k prenosu jeho údajov do tretej krajiny, ktorá neposkytuje primeranú ochranu v zmysle [smernice 95/46];

g) postúpi akékoľvek oznámenie prijaté od vývozcu údajov alebo subdodávateľa podľa doložky 5 písm. b) a doložky 8 ods. 3 dozornému orgánu na ochranu údajov, pokiaľ sa vývozca údajov rozhodne pokračovať v prenose alebo zrušiť jeho pozastavenie;

…“

35 Doložka 5 uvedenej prílohy, nazvaná „Povinnosti vývozcu [dovozcu – *neoficiálny preklad*] údajov…“, stanovuje:

„Dovozca údajov sa zaväzuje a zaručuje, že:

a) bude spracovávať osobné údaje iba v mene vývozcu údajov a v súlade s jeho pokynmi a doložkami; ak z akýchkoľvek dôvodov nebude môcť toto dodržiavanie pokynov a doložiek zabezpečiť, zaväzuje sa bezodkladne o tom informovať vývozcu údajov, ktorý je v takom prípade oprávnený pozastaviť prenos údajov a/alebo zmluvu vypovedať;

b) nemá dôvod sa domnievať, že právne predpisy, ktorým podlieha, mu bránia plniť pokyny vývozcu údajov a jeho záväzky vyplývajúce zo zmluvy a že v prípade zmeny týchto právnych predpisov, ktorá by mohla mať závažný nepriaznivý účinok na záruky a záväzky stanovené doložkami, bezodkladne oznámi túto zmenu vývozcovi údajov, ktorý je v takom prípade oprávnený pozastaviť prenos údajov a/alebo zmluvu vypovedať;

…

d) vývozcovi údajov bezodkladne oznámi:
   i) akékoľvek právne záväzné požiadavky na sprístupnenie osobných údajov zo strany orgánu presadzovania práva, pokiaľ to nie je inak zakázané, napríklad trestným právom, v záujme zachovania dôvernosti vyšetrovania v rámci presadzovania práva;
   ii) akýkoľvek neúmyselný alebo neoprávnený prístup a
   iii) akékoľvek požiadavky pochádzajúce priamo od subjektov údajov bez toho, aby na tieto požiadavky reagoval s výnimkou prípadu, ak je tým inak poverený;

…“

36 V poznámke pod čiarou, na ktorú odkazuje názov tejto doložky 5, sa uvádza:

„Povinné požiadavky vnútroštátnych právnych predpisov vzťahujúcich sa na dovozcu údajov, ktoré nepresahujú rámec toho, čo je nevyhnutné v demokratickej spoločnosti na základe jedného zo záujmov uvedených v článku 13 ods. 1 smernice [95/46], t. j. ak predstavujú opatrenia nevyhnutné na zabezpečenie obrany národnej bezpečnosti, verejnej bezpečnosti, na predchádzanie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo porušenie etických zásad regulovaných profesií, významného hospodárskeho alebo finančného záujmu štátu alebo ochrany subjektov údajov alebo práv a slobôd iných, nie sú v rozpore so štandardnými zmluvnými doložkami. …“

37 Doložka 6 prílohy rozhodnutia 2010/87 s názvom „Zodpovednosť“ stanovuje:

„1. Strany sa dohodli že subjekt údajov, ktorý utrpel škodu v dôsledku porušenia povinností uvedených v doložke 3 alebo doložke 11 spôsobeného ktoroukoľvek zo strán alebo subdodávateľom, má nárok na odškodnenie od vývozcu údajov.

2. Ak subjekt údajov nemôže v súlade s odsekom 1 požadovať odškodnenie od vývozcu údajov za porušenie niektorej z povinností dovozcu údajov alebo jeho subdodávateľa uvedených v doložke 3 alebo doložke 11, pretože vývozca údajov fakticky zmizol, prestal právne existovať alebo sa stal platobne neschopným, dovozca údajov sa zaväzuje, že subjekt údajov smie uplatňovať nároky voči dovozcovi údajov, ako by bol vývozcom údajov…

…“

38 Doložka 8 tejto prílohy, nazvaná „Spolupráca s dozornými orgánmi“, v odseku 2 stanovuje:

„Strany súhlasia, že dozorný orgán má právo vykonať audit dovozcu údajov alebo akéhokoľvek subdodávateľa v rovnakom rozsahu a za rovnakých podmienok, aké by sa uplatňovali pri audite vývozcu údajov v súlade s príslušným právom týkajúcim sa ochrany údajov.“

39 Doložka 9 uvedenej prílohy, nazvaná „Rozhodné právo“, spresňuje, že doložky sa majú riadiť právom členského štátu, v ktorom je vývozca údajov usadený.

40 Podľa doložky 11 tej istej prílohy, nazvanej „Spracovanie údajov subdodávateľmi“:

„1. Dovozca údajov nezadá na spracovanie subdodávateľom žiadnu zo spracovateľských operácií, ktoré vykonáva v mene vývozcu údajov podľa doložiek, bez predchádzajúceho písomného súhlasu vývozcu údajov. Pokiaľ dovozca údajov so súhlasom vývozcu údajov zadáva zákazky na spracovanie údajov subdodávateľom podľa doložiek, môže to uskutočniť len formou písomnej dohody so subdodávateľom, ktorá subdodávateľovi uloží rovnaké záväzky, aké má dovozca údajov podľa doložiek…

2. Predchádzajúca písomná zmluva medzi dovozcom údajov a subdodávateľom má tiež ustanoviť doložku o oprávnenosti tretej strany, ako je uvedené v doložke 3, pre tie prípady, keď subjekt údajov nemôže požadovať odškodnenie podľa odseku 1 doložky 6 od vývozcu údajov alebo dovozcu údajov,

pretože fakticky zmizli alebo prestali právne existovať, alebo sa stali platobne neschopnými a žiaden nástupnícky subjekt neprevzal na základe zmluvy alebo podľa zákona všetky právne záväzky vývozcu údajov. Táto zodpovednosť subdodávateľa voči tretím stranám je obmedzená na jeho vlastné operácie súvisiace so spracovaním údajov podľa doložiek.

…“

41 Doložka 12, nazvaná „Povinnosti po ukončení poskytovania služieb spojených so spracovaním osobných údajov“, v odseku 1 stanovuje:

„Strany sa dohodli, že po ukončení poskytovania služieb spojených so spracovaním údajov dovozca údajov a subdodávateľ podľa rozhodnutia vývozcu údajov vráti všetky prenášané osobné údaje a ich kópie vývozcovi údajov alebo zničí všetky osobné údaje a predloží vývozcovi potvrdenie o ich zničení, pokiaľ právne predpisy vzťahujúce sa na dovozcu údajov nezakazujú dovozcovi vrátenie alebo zničenie všetkých alebo časti prenášaných osobných údajov. …“

Rozhodnutie ŠnOOÚ

42 Rozsudkom zo 6. októbra 2015, Schrems (C-362/14, EU:C:2015:650), Súdny dvor zrušil rozhodnutie Komisie 2000/520/ES z 26. júla 2000 v súlade so smernicou 95/46 o primeranosti ochrany poskytovanej zásadami bezpečného prístavu a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu Spojených štátov amerických, ktorým Európska komisia konštatovala, že táto tretia krajina zaručuje primeranú úroveň ochrany.

43 Po vyhlásení tohto rozsudku Komisia prijala rozhodnutie ŠnOOÚ, na čo musela najskôr vykonať posúdenie právnej úpravy Spojených štátov, ako to spresňuje odôvodnenie 65 uvedeného rozhodnutia:

„Komisia posúdila obmedzenia a záruky, ktoré sú k dispozícii v rámci práva USA v súvislosti s prístupom k osobným údajom prenášaným v rámci štítu na ochranu osobných údajov medzi [Európskou úniou] a USA orgánmi verejnej moci USA na účely národnej bezpečnosti, presadzovania práva a iné účely verejného záujmu a s ich používaním. Vláda USA navyše prostredníctvom svojho Úradu riaditeľa národnej spravodajskej služby (Office of the Director of National Intelligence – ODNI)… poskytla Komisii podrobné vyhlásenia a záväzky, ktoré sú uvedené v prílohe VI k tomuto rozhodnutiu. Listom podpísaným ministrom zahraničných vecí a priloženým ako príloha III k tomuto rozhodnutiu sa vláda USA takisto zaviazala vytvoriť nový mechanizmus dohľadu nad zásahmi na účely národnej bezpečnosti, a to funkciu ombudsmana pre štít na ochranu osobných údajov, ktorý je nezávislý od spravodajských služieb (Intelligence Community). A napokon, vo vyhlásení Ministerstva spravodlivosti USA uvedeného v prílohe VII k tomuto rozhodnutiu sa opisujú obmedzenia a záruky vzťahujúce sa na prístup k údajom a ich používanie orgánmi verejnej moci na účely presadzovania práva a iné účely verejného záujmu. V záujme zvýšenia transparentnosti a ako výraz právnej povahy týchto záväzkov sa všetky uvedené dokumenty priložené k tomuto rozhodnutiu uverejnia vo Federálnom registri USA.“

44 Analýza Komisie týkajúca sa týchto obmedzení a záruk je zhrnutá v odôvodneniach 67 až 135 rozhodnutia ŠnOOÚ, zatiaľ čo závery tejto inštitúcie týkajúce sa primeranej úrovne ochrany v rámci štítu na ochranu osobných údajov Európskej únie – Spojené štáty sú uvedené v odôvodneniach 136 až 141 tohto rozhodnutia.

45 Konkrétne odôvodnenia 68, 69, 76, 77, 109, 112 až 116, 120, 136 a 140 tohto rozhodnutia stanovujú:

„(68) Podľa ústavy USA patrí zabezpečenie národnej bezpečnosti do právomoci prezidenta ako vrchného veliteľa, najvyššieho predstaviteľa výkonnej moci, a, pokiaľ ide o zahraničné spravodajstvo, ako osoby, ktorá vykonáva zahraničnú politiku USA… Hoci Kongres má

právomoc ukladať obmedzenia a robí to v rôznych ohľadoch, prezident môže v rámci týchto hraníc usmerňovať činnosť spravodajských služieb USA, a to najmä prostredníctvom vykonávacích nariadení alebo prezidentských smerníc. … V súčasnosti sú dva ústredné právne nástroje v tomto ohľade vykonávacie nariadenie č. 12333 [*Executive Order 12333*, ďalej len ‚E.O. 12333']… a prezidentská politická smernica 28 [*Presidential Policy directive 28*, ďalej len ‚PPD-28'].

(69) V [PPD-28] vydanej 17. januára 2014 sa ukladá niekoľko obmedzení operácií ‚signálového spravodajstva'… Táto prezidentská smernica je právne záväzná pre spravodajské orgány USA… a zostane účinná aj po zmene vlády v USA… Prezidentská politická smernica 28 má osobitný význam pre osoby, ktoré nie sú občanmi ani rezidentmi USA, vrátane dotknutých osôb z EÚ. …

…

(76) Hoci tieto zásady [PPD-28] nie sú formulované v týchto právnych pojmoch, zachytávajú podstatu zásad nevyhnutnosti a proporcionality. …

(77) Tieto požiadavky vydané vo forme smernice prezidenta ako najvyššieho predstaviteľa výkonnej moci sú záväzné pre všetky spravodajské služby a ďalej sa uplatňujú prostredníctvom pravidiel a postupov agentúr, ktorými sa transponujú všeobecné zásady do konkrétnych pokynov na každodenné operácie. …

…

(109) Naopak, podľa oddielu 702 zákona [Foreign Intelligence Surveillance Act (FISA)] súd [United States Foreign Intelligence Surveillance Court (FISC) (súd pre sledovanie v rámci zahraničného spravodajstva)]… nepovoľuje jednotlivé opatrenia sledovania; povoľuje skôr programy sledovania (ako PRISM, UPSTREAM) na základe každoročných certifikácií pripravených generálnym prokurátorom [United States Attorney General] a riaditeľom národnej spravodajskej služby [Director of National Intelligence (DNI)]…… Ako bolo uvedené, certifikácie, ktoré schvaľuje súd FISC, neobsahujú žiadne informácie o jednotlivých osobách, ktoré majú byť zacielené, ale identifikujú kategórie zahraničných spravodajských informácií… Hoci súd FISC neposudzuje – na základe pravdepodobnej príčiny alebo inej normy –, či boli osoby správne zacielené s cieľom získať zahraničné spravodajské informácie…, jeho kontrola sa vzťahuje na podmienku, že ‚významným účelom získavania údajov je získať zahraničné spravodajské informácie'…

…

(112) Po prvé zákon o sledovaní v rámci zahraničného spravodajstva obsahuje viacero opravných prostriedkov aj pre osoby, ktoré nie sú občanmi ani rezidentmi USA, proti nezákonnému elektronickému sledovaniu… Fyzické osoby majú možnosť podať občianskoprávnu žalobu o peňažné odškodné proti USA, keď boli informácie o nich nezákonne a úmyselne použité alebo zverejnené…; žalovať osobne úradníkov vlády USA (za protiprávne konanie ‚pod zámienkou zákona') o peňažné odškodné…; a napadnúť zákonnosť sledovania (s cieľom utajiť informácie) v prípade, že vláda USA chce použiť alebo zverejniť akékoľvek informácie získané alebo odvodené z elektronického sledovania jednotlivcov v súdnom alebo správnom konaní v USA…

(113) Po druhé, vláda USA informovala Komisiu o niekoľkých ďalších možnostiach, ktoré dotknuté osoby z EÚ môžu využiť v snahe uplatniť opravný prostriedok proti úradníkom vlády za nezákonný prístup vlády k osobným údajom alebo za ich používanie, a to aj na údajné účely národnej bezpečnosti…

(114) A napokon, vláda USA poukazuje na zákon [Freedom of information Act (FOIA) (zákon o slobodnom prístupe k informáciám)] ako na prostriedok pre osoby, ktoré nie sú občanmi ani rezidentmi USA, ako požiadať o prístup k existujúcim záznamom federálnej agentúry vrátane prípadov, keď obsahujú osobné údaje fyzickej osoby… Vzhľadom na svoje zameranie zákon FOIA neposkytuje možnosť individuálnej nápravy proti zásahom do osobných údajov ako takým, aj keď by v zásade mohol umožniť fyzickým osobám získať prístup k relevantným informáciám držaným národnými spravodajskými agentúrami. …

(115) Hoci teda fyzické osoby vrátane dotknutých osôb z EÚ majú niekoľko možností nápravy, keď sa stali predmetom nezákonného (elektronického) sledovania na účely národnej bezpečnosti, je jasné aj to, že tieto možnosti sa nevzťahujú aspoň na niektoré právne základy, ktoré spravodajské orgány USA môžu využiť (napr. vykonávacie nariadenie [E.O.] č. 12333). Navyše aj v tých prípadoch, keď v zásade existujú možnosti súdnej nápravy pre osoby, ktoré nie občanmi ani rezidentmi USA, napríklad v prípade sledovania na základe zákona FISA, sú dostupné dôvody žaloby obmedzené…, pretože žaloby podané fyzickými osobami (vrátane občanov a rezidentov USA) budú vyhlásené za neprípustné, ak nedokážu preukázať „aktívnu legitimáciu“ …, čo obmedzuje prístup k všeobecným súdom…

(116) S cieľom poskytnúť ďalšiu možnosť nápravy prístupnú pre všetky dotknuté osoby z EÚ sa vláda USA rozhodla vytvoriť nový mechanizmus ombudsmana, ako je uvedené v liste ministra zahraničných vecí USA Komisii, ktorý sa nachádza v prílohe III k tomuto rozhodnutiu. Tento mechanizmus nadväzuje na určenie vysokého koordinátora (na úrovni tajomníka ministra) na ministerstve zahraničných vecí podľa [PPD-28], ktorý je kontaktnou osobou pre zahraničné vlády na vyjadrenie obáv v súvislosti s činnosťou USA v oblasti signálového spravodajstva, ale značne presahuje túto pôvodnú koncepciu.

…

(120) … Vláda USA sa zaväzuje, že zaistí, aby sa ombudsman pre štít na ochranu osobných údajov pri vykonávaní svojich funkcií mohol spoľahnúť na spoluprácu v rámci iných mechanizmov dohľadu a preskúmania dodržiavania predpisov, ktoré existujú v práve USA. … Ak jeden z týchto orgánov dohľadu zistí akékoľvek nedodržanie predpisov, daná zložka spravodajských služieb (napríklad spravodajská agentúra) bude musieť toto nedodržanie pravidiel napraviť, pretože len tak sa umožní ombudsmanovi poskytnúť ‚kladnú‘ odpoveď danej fyzickej osobe (t. j. že došlo k náprave každého nedodržania predpisov), k čomu sa vláda USA zaviazala. …

…

(136) Na základe týchto zistení sa Komisia domnieva, že USA zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám v USA, ktoré osvedčili svoje dodržiavanie zásad, v rámci štítu na ochranu osobných údajov medzi [Európskou úniou] a USA.

…

(140) A napokon, na základe dostupných informácií o právnom poriadku USA vrátane vyhlásení a záväzkov vlády USA sa Komisia domnieva, že akékoľvek zásahy orgánov verejnej moci USA do základných práv osôb, ktorých údaje sa prenášajú z Únie do USA v rámci štítu na ochranu osobných údajov na účely národnej bezpečnosti, presadzovania práva alebo iných verejných záujmov, a následné obmedzenia organizácií, ktoré osvedčili svoje dodržiavanie zásad, s ohľadom na to, ako dodržiavajú zásady, budú obmedzené na to, čo je nevyhnutne potrebné na dosiahnutie príslušného legitímneho cieľa, a že existuje účinná právna ochrana pred takými zásahmi.“

46 V zmysle článku 1 rozhodnutia ŠnOOÚ:

„1. Na účely článku 25 ods. 2 [smernice 95/46] Spojené štáty zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám v USA v rámci štítu na ochranu osobných údajov medzi [Európskou úniou] a USA.

2. Štít na ochranu osobných údajov medzi [Európskou úniou] a USA tvoria zásady vydané Ministerstvom obchodu USA 7. júla 2016, ktoré sú uvedené v prílohe II, a oficiálne vyhlásenia a záväzky obsiahnuté v dokumentoch uvedených v prílohách I, III až VII.

3. Na účely odseku 1 sa osobné údaje prenášajú v rámci štítu na ochranu osobných údajov medzi [Európskou úniou] a USA, keď sa prenášajú z Únie organizáciám v USA, ktoré sú zahrnuté do ‚zoznamu organizácií zapojených do štítu na ochranu osobných údajov', ktorý vedie a sprístupňuje verejnosti Ministerstvo obchodu USA v súlade s oddielmi I a III zásad stanovených v prílohe II."

47 Príloha II rozhodnutia ŠnOOÚ, nazvaná „Zásady rámca štítu na ochranu osobných údajov medzi [Európskou úniou] a USA vydané ministerstvom obchodu USA", vo svojom bode I.5. stanovuje, že dodržiavanie zásad môže byť obmedzené najmä „môže byť obmedzené najmä požiadavk[ami] národnej bezpečnosti, verejného záujmu [a] presadzovania práva".

48 Príloha III tohto rozhodnutia obsahuje list od pána Johna Kerryho, vtedajšieho Secretary of State (minister zahraničných vecí, Spojené štáty), zaslaný komisárke pre spravodlivosť, spotrebiteľov a rodovú rovnosť, zo 7. júla 2016, ku ktorému je v prílohe A pripojené memorandum s názvom „Mechanizmus ombudsmana pre štít na ochranu osobných údajov medzi EÚ a USA týkajúci sa signálového spravodajstva", ktoré obsahuje tento text:

„Uznávajúc význam rámca štítu na ochranu osobných údajov medzi [Európskou úniou] a USA sa týmto memorandom stanovuje postup zavedenia nového mechanizmu týkajúceho sa signálového spravodajstva, ktorý je v súlade s… PPD-28…

… Prezident Obama oznámil vydanie novej prezidentskej smernice PPD-28, ktorá ‚jasne stanoví, čo robíme a čo nerobíme, pokiaľ ide o naše zahraničné sledovanie'.

V oddiele 4 písm. d) smernice PPD-28 sa nariaďuje ministrovi zahraničných vecí, aby vymenoval ‚hlavného koordinátora medzinárodnej diplomacie v oblasti informačných technológií' (ďalej len ‚hlavný koordinátor'), ktorý by mal ‚slúžiť ako kontaktná osoba pre zahraničné vlády, ktoré chcú vyjadriť znepokojenie týkajúce sa činností signálového spravodajstva Spojených štátov'.

…

1. [Hlavný koordinátor]… bude slúžiť ako ombudsman pre štít na ochranu osobných údajov a… bude úzko spolupracovať s poverenými úradníkmi z iných ministerstiev a agentúr, ktorí sú zodpovední za spracovávanie žiadostí v súlade s platnými právnymi predpismi a politikami Spojených štátov. Ombudsman nie je závislý od spravodajských služieb. Ombudsman podlieha priamo ministrovi zahraničných vecí, ktorý zabezpečí, aby ombudsman vykonával svoju funkciu objektívne a bez pôsobenia neprimeraných vplyvov, ktoré by mohli viesť k ovplyvňovaniu poskytovanej odpovede.

…"

49 Príloha VI rozhodnutia ŠnOOÚ obsahuje list od Úradu riaditeľa národnej spravodajskej služby (Office of the Director of National Intelligence) Ministerstvu obchodu USA, ako aj správnemu orgánu zahraničného obchodu z 21. júna 2016, v ktorom sa uvádza, že PPD-28 umožňuje „hromadné

zhromažďovanie‘… pomerne veľkého objemu informácií alebo údajov prostredníctvom signálového spravodajstva za okolností, keď spravodajské služby nemôžu použiť identifikátor spojený s konkrétnym cieľom…, aby mohli presne zamerať zhromažďovanie informácií“.

Spor vo veci samej a prejudiciálne otázky

50 Pán Schrems, rakúsky štátny príslušník s bydliskom v Rakúsku, je používateľom sociálnej siete Facebook (ďalej len „Facebook“) od roku 2008.

51 Každý, kto má bydlisko na území Únie a chce používať Facebook, musí v rámci svojej registrácie uzavrieť zmluvu so spoločnosťou Facebook Ireland, dcérskou spoločnosťou Facebook Inc., ktorá má sídlo v Spojených štátoch. Osobné údaje klientov spoločnosti Facebook s bydliskom na území Únie sa v celom rozsahu alebo sčasti prenášajú na servery patriace spoločnosti Facebook Inc., ktoré sa nachádzajú na území Spojených štátov, kde sa spracúvajú.

52 Dňa 25. júna 2013 sa pán Schrems obrátil na komisára so sťažnosťou, v ktorej ho v podstate žiadal, aby zakázal spoločnosti Facebook Ireland prenos jeho osobných údajov do Spojených štátov, pričom tvrdil, že platné právo a prax v tejto krajine nezaručujú dostatočnú ochranu osobných údajov uchovávaných na jej území pred činnosťami sledovania, ktoré tam vykonávali orgány verejnej moci. Táto sťažnosť bola zamietnutá najmä z dôvodu, že Komisia vo svojom rozhodnutí 2000/520 konštatovala, že Spojené štáty zabezpečovali primeranú úroveň ochrany.

53 High Court (Vyšší súd, Írsko), na ktorý pán Schrems podal žalobu proti zamietnutiu jeho sťažnosti, podal na Súdny dvor návrh na začatie prejudiciálneho konania týkajúci sa výkladu a platnosti rozhodnutia 2000/520. Rozsudkom zo 6. októbra 2015, Schrems (C-362/14, EU:C:2015:650), Súdny dvor vyhlásil toto rozhodnutie za neplatné.

54 V nadväznosti na tento rozsudok vnútroštátny súd zrušil zamietnutie sťažnosti pána Schremsa a vrátil ju komisárovi. V rámci konania, ktoré tento orgán začal, Facebook Ireland vysvetlila, že veľká časť osobných údajov bola prenesená na spoločnosť Facebook Inc. na základe štandardných doložiek o ochrane údajov uvedených v prílohe rozhodnutia 2010/87. Vzhľadom na tieto skutočnosti komisár vyzval pána Schremsa, aby svoju sťažnosť preformuloval.

55 Vo svojej v tomto zmysle preformulovanej sťažnosti podanej 1. decembra 2015 pán Schrems najmä tvrdil, že americké právo ukladá spoločnosti Facebook Inc. povinnosť sprístupniť osobné údaje, ktoré sú jej prenesené, americkým orgánom, akými sú National Security Agency (NSA) a Federal Bureau of Investigation (FBI). Tvrdil, že vzhľadom na to, že tieto údaje boli použité v rámci rôznych programov sledovania spôsobom nezlučiteľným s článkami 7, 8 a 47 Charty, rozhodnutie 2010/87 nemôže odôvodniť prenos uvedených údajov do Spojených štátov. Za týchto podmienok pán Schrems požiadal komisára, aby zakázal alebo pozastavil prenos jeho osobných údajov na spoločnosť Facebook Inc.

56 Dňa 24. mája 2016 komisár uverejnil „návrh rozhodnutia“, v ktorom zhrnul predbežné závery svojho vyšetrovania. V tomto návrhu predbežne konštatoval, že k osobným údajom občanov Únie prenášaným do Spojených štátov možno pristupovať a spracúvať ich orgánmi Spojených štátov spôsobom nezlučiteľným s článkami 7 a 8 Charty a že právo Spojených štátov neposkytuje týmto občanom opravné prostriedky zlučiteľné s článkom 47 Charty. Komisár sa domnieval, že štandardné doložky o ochrane údajov pripojené k rozhodnutiu 2010/87 nemôžu napraviť tento nedostatok, keďže dotknutým osobám priznávajú len zmluvné práva voči vývozcovi a dovozcovi údajov, avšak bez toho, aby zaväzovali americké orgány.

57 Keďže sa za týchto podmienok komisár domnieval, že preformulovaná sťažnosť pána Schremsa nastoľovala otázku platnosti rozhodnutia 2010/87, 31. mája 2016 sa obrátil na High Court (Vyšší súd), pričom poukazoval na judikatúru vyplývajúcu z rozsudku zo 6. októbra 2015, Schrems (C-362/14,

EU:C:2015:650, bod 65), aby sa tento súd obrátil na Súdny dvor s touto otázkou. Rozhodnutím zo 4. mája 2018 High Court (Vyšší súd) podal prejednávaný návrh na začatie prejudiciálneho konania na Súdny dvor.

58 High Court (Vyšší súd) pripojil k tomuto návrhu na začatie prejudiciálneho konania rozsudok vyhlásený 3. októbra 2017, v ktorom uviedol výsledok preskúmania dôkazov, ktoré mu boli predložené v rámci vnútroštátneho konania, teda konania, na ktorom sa zúčastnila americká vláda.

59 V uvedenom rozsudku, na ktorý sa viackrát odvoláva návrh na začatie prejudiciálneho konania, vnútroštátny súd uviedol, že v zásade má nielen právo, ale aj povinnosť preskúmať všetky skutočnosti a tvrdenia, ktoré mu boli predložené, aby na ich základe rozhodol, či je alebo nie je potrebné podať návrh na začatie prejudiciálneho konania. V každom prípade je povinný zohľadniť prípadné zmeny práva, ku ktorým došlo medzi podaním žaloby a pojednávaním, ktoré pred ním prebiehalo. Tento súd spresnil, že v rámci veci samej sa jeho vlastné posúdenie neobmedzuje na dôvody neplatnosti uvádzané komisárom, takže môže odhaliť aj *ex offo* iné dôvody neplatnosti a na ich základe podať návrh na začatie prejudiciálneho konania.

60 Podľa konštatovaní uvedených v danom rozsudku sa spravodajské činnosti orgánov Spojených štátov, pokiaľ ide o osobné údaje prenášané do Spojených štátov, zakladajú najmä na článku 702 FISA a E.O. 12333.

61 Pokiaľ ide o článok 702 FISA, vnútroštátny súd v tom istom rozsudku spresnil, že tento článok umožňuje generálnemu prokurátorovi a riaditeľovi národnej spravodajskej služby, aby po schválení FISC s cieľom získať „zahraničné spravodajské informácie“ spoločne povolili sledovanie osôb, ktoré nie sú americkými občanmi a ktoré sa nenachádzajú na území Spojených štátov, a slúži najmä ako základ pre programy sledovania PRISM a UPSTREAM. V rámci programu PRISM sú poskytovatelia internetových služieb, ako konštatuje tento súd, povinní poskytnúť NSA celú zasielanú a prijímanú komunikáciu „selektora“, pričom časť z nich sa posiela aj FBI a Central Intelligence Agency (CIA) (Ústredná spravodajská služba).

62 Pokiaľ ide o program UPSTREAM, uvedený súd konštatoval, že v rámci tohto programu sú telekomunikačné podniky prevádzkujúce „chrbtovú“ sieť, t. j. sieť káblov, prepínačov a smerovačov povinné umožniť NSA kopírovať a filtrovať internetovú komunikáciu na účely zhromažďovania komunikácie zaslanej, prijatej alebo týkajúcej sa osoby, ktorá nie je americkým občanom ani rezidentom, a ktorú vyberie „selektor“. V rámci uvedeného programu má NSA podľa zistení tohto súdu prístup tak k metaúdajom, ako aj k obsahu predmetných komunikácií.

63 Pokiaľ ide o E.O. 12333, vnútroštátny súd konštatuje, že umožňuje NSA prístup k údajom nachádzajúcim sa „na ceste“ do Spojených štátov prostredníctvom prístupu k podmorským káblom uloženým na dne Atlantického oceánu, ako aj získavanie a uchovávanie týchto údajov pred ich vstupom do Spojených štátov a uplatňovaním tam na ne ustanovenia zákona FISA. Spresňuje, že činnosti založené na E.O. 12333 sa nespravujú zákonom.

64 Pokiaľ ide o obmedzenia spravodajských činností, vnútroštátny súd kladie dôraz na skutočnosť, že osoby, ktoré nie sú americkými občanmi ani rezidentmi, spadajú výlučne pod PPD-28 a že táto smernica len uvádza, že spravodajské činnosti by mali byť „v čo najväčšej uskutočniteľnej miere prispôsobené [čo možno najpresnejšie zacielené – *neoficiálny preklad*]“ (*as tailored as feasible*). Na základe týchto konštatovaní sa uvedený súd domnieva, že Spojené štáty vykonávajú hromadné spracúvanie osobných údajov bez toho, aby zabezpečili úroveň ochrany v podstate rovnocennú tej, ktorá je zaručená článkami 7 a 8 Charty.

65 Pokiaľ ide o súdnu ochranu, ten istý súd uvádza, že občania Únie nemajú prístup k rovnakým prostriedkom nápravy, aké majú americkí štátni príslušníci proti spracúvaniu osobných údajov americkými orgánmi, keďže štvrtý dodatok ku Constitution of the United States (Ústava Spojených

štátov), ktorá v americkom práve predstavuje najdôležitejšiu ochranu pred nezákonným sledovaním, sa nevzťahuje na občanov Únie. V tejto súvislosti vnútroštátny súd spresňuje, že žaloby, ktoré majú títo občania k dispozícii, narážajú na značné prekážky, najmä na povinnosť – podľa jeho názoru príliš ťažko splniteľnú – preukázať svoju aktívnu legitimáciu. Okrem toho z jeho konštatovaní vyplýva, že činnosti NSA založené na E.O. 12333 nemôžu byť predmetom súdneho preskúmania a nemožno proti nim podať opravný prostriedok. Uvedený súd sa napokon domnieva, že vzhľadom na to, že podľa jeho názoru ombudsman pre štít na ochranu údajov nepredstavuje súd v zmysle článku 47 Charty, americké právo nezaručuje občanom Únie úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej základným právom zakotveným v tomto článku.

66 Vnútroštátny súd vo svojom návrhu na začatie prejudiciálneho konania ďalej spresňuje, že spor medzi účastníkmi konania vo veci samej sa týka najmä otázky uplatniteľnosti práva Únie na prenosy osobných údajov do tretej krajiny, ktoré môžu byť spracúvané orgánmi tejto krajiny najmä na účely národnej bezpečnosti, ako aj skutočností, ktoré treba zohľadniť na účely posúdenia primeranosti úrovne ochrany zabezpečovanej uvedenou krajinou. Tento súd konkrétne uvádza, že podľa spoločnosti Facebook Ireland zistenia Komisie týkajúce sa primeranosti úrovne ochrany zabezpečovanej treťou krajinou, akými sú zistenia uvedené v rozhodnutí ŠnOOÚ, zaväzujú dozorné orgány aj v kontexte prenosu osobných údajov založeného na štandardných doložkách o ochrane údajov uvedených v prílohe rozhodnutia 2010/87.

67 Pokiaľ ide o tieto štandardné doložky o ochrane údajov, daný súd sa pýta, či rozhodnutie 2010/87 možno považovať za platné, hoci podľa toho istého súdu uvedené doložky nemajú pre štátne orgány dotknutej tretej krajiny záväzný charakter, a preto nemôžu napraviť prípadnú neexistenciu primeranej úrovne ochrany v uvedenej krajine. V tejto súvislosti sa domnieva, že možnosť zakázať prenosy osobných údajov do tretej krajiny, ktorá dovozcovi ukladá povinnosti nezlučiteľné so zárukami obsiahnutými v tých istých ustanoveniach, ktorú príslušným orgánom členských štátov priznáva článok 4 ods. 1 písm. a) rozhodnutia 2010/87 v znení predchádzajúcom nadobudnutiu účinnosti vykonávacieho rozhodnutia 2016/2297, preukazuje, že právny stav v tretej krajine môže byť dôvodom pre zákaz prenosu údajov, aj vtedy, keď sa uskutočňuje na základe štandardných doložiek o ochrane údajov, ktoré sú uvedené v prílohe rozhodnutia 2010/87, a teda je zjavné, že tieto doložky môžu byť neprimerané na zabezpečenie primeranej ochrany. Za týchto okolností sa vnútroštátny súd pýta na rozsah právomoci komisára zakázať prenos údajov založený na týchto doložkách, pričom sa domnieva, že diskrečná právomoc nemôže stačiť na zabezpečenie primeranej ochrany.

68 Za týchto podmienok High Court (Vyšší súd) rozhodol prerušiť konanie a položiť Súdnemu dvoru tieto prejudiciálne otázky:

„1. V situácii, keď súkromná spoločnosť prenáša osobné údaje z členského štátu [Únie] súkromnej spoločnosti v tretej krajine na komerčné účely podľa [rozhodnutia 2010/87] a [tieto] môžu byť ďalej spracúvané v tretej krajine jej orgánmi na účely národnej bezpečnosti, ale aj na účely presadzovania práva a plnenia úloh zahraničných vecí uvedenej tretej krajiny, uplatňuje sa právo [Únie], vrátane Charty, na prenos týchto údajov bez ohľadu na ustanovenia článku 4 ods. 2 ZEÚ vo vzťahu k národnej bezpečnosti a ustanovenia prvej zarážky článku 3 ods. 2 [smernice 95/46] vo vzťahu k verejnej bezpečnosti, obrane a bezpečnosti štátu?

2. a) Pri určovaní toho, či prenosom údajov z [Únie] do tretej krajiny na základe rozhodnutia [2010/87], v ktorej sa môžu ďalej spracúvať na účely národnej bezpečnosti, došlo k porušeniu práv fyzickej osoby, je príslušným porovnávacím prostriedkom na účely [95/46] smernice:
   i) Charta, Zmluva EÚ, Zmluva o FEÚ, smernica [95/46], [Európsky dohovor o ochrane ľudských práv a základných slobôd, podpísaný v Ríme 4. novembra 1950] (alebo iné ustanovenie práva [Únie]); alebo
   ii) vnútroštátne právne predpisy jedného alebo viacerých členských štátov?

b) Ak je príslušným porovnávacím prostriedkom bod ii), majú byť do porovnávacieho prostriedku zahrnuté aj postupy v kontexte národnej bezpečnosti v jednom alebo viacerých členských štátoch?

3. Pri posudzovaní toho, či tretia krajina zabezpečuje úroveň ochrany vyžadovanú právnymi predpismi [Únie] pre osobné údaje prenášané do tejto krajiny na účely článku 26 smernice [95/46], mala by sa úroveň ochrany v tejto tretej krajine posudzovať na základe:
   a) platných pravidiel v tejto tretej krajine vyplývajúcich z jej vnútroštátnych právnych predpisov alebo medzinárodných záväzkov a praxe určenej na zabezpečenie súladu s týmito pravidlami, vrátane odborných pravidiel a bezpečnostných opatrení, ktoré sa v tejto tretej krajine dodržiavajú;

      alebo
   b) pravidiel uvedených v písmene a) spolu s takými administratívnymi a regulačnými postupmi a postupmi v oblasti dodržiavania právnych predpisov, a zárukami vyplývajúcimi zo zásad, postupmi, protokolmi, mechanizmami dohľadu a mimosúdnymi prostriedkami nápravy, ktoré existujú v tejto tretej krajine?

4. Vzhľadom na skutočnosti zistené High Court (Vyšší súd) vo vzťahu k právnym predpisom Spojených štátov amerických, ak sa osobné údaje prenášajú z [Únie] do USA na základe rozhodnutia [2010/87], porušuje to práva fyzickej osoby podľa článkov 7 alebo 8 Charty?

5. Vzhľadom na skutočnosti zistené High Court (Vyšší súd) vo vzťahu k právnym predpisom Spojených štátov amerických, ak sa osobné údaje prenášajú z [Únie] do USA na základe rozhodnutia [2010/87]:
   a) rešpektuje úroveň ochrany, ktorú poskytujú USA, podstatu práva fyzickej osoby na súdny prostriedok nápravy za porušenie jej práv na ochranu osobných údajov, zaručený článkom 47 Charty?

      Ak je odpoveď na písmeno a) kladná,
   b) sú obmedzenia vyplývajúce z právnych predpisov Spojených štátov amerických pre právo fyzickej osoby na súdny prostriedok nápravy v kontexte americkej národnej bezpečnosti primerané v zmysle článku 52 Charty a nevymykajú sa rámcu toho, čo je v demokratickej spoločnosti nevyhnutné na účely národnej bezpečnosti?

6. a) Aká je úroveň ochrany, ktorú je potrebné poskytnúť osobným údajom prenášaným do tretej krajiny na základe štandardných zmluvných doložiek prijatých v súlade s rozhodnutím Komisie podľa článku 26 ods. 4 smernice [95/46] v spojení s ustanoveniami [tejto smernice] a najmä podľa [jej] článkov 25 a 26 v spojení s Chartou?
   b) Ktoré záležitosti je potrebné zohľadniť pri posudzovaní toho, či úroveň ochrany poskytnutá údajom prenášaným do tretej krajiny na základe rozhodnutia [2010/87] spĺňa požiadavky smernice [95/46] a Charty?

7. Vylučuje skutočnosť, že štandardné doložky o ochrane údajov platia medzi vývozcom údajov a dovozcom údajov a nezaväzujú vnútroštátne orgány tretej krajiny, ktoré môžu od dovozcu údajov požadovať, aby sprístupnil ich bezpečnostným službám na ďalšie spracúvanie osobné údaje prenesené podľa ustanovení upravených v rozhodnutí [2010/87], aby doložky poskytovali primerané záruky, ako to predpokladá článok 26 ods. 2 smernice [95/46]?

8. Ak dovozca údajov z tretej krajiny podlieha právnym predpisom o dohľade, ktoré sú podľa názoru úradu na ochranu údajov v rozpore so štandardnými doložkami o ochrane údajov alebo článkami 25 a 26 smernice [95/46] alebo Charty, je úrad na ochranu údajov povinný využiť svoje právomoci na presadzovanie práva podľa článku 28 ods. 3 smernice [95/46] na prerušenie toku

údajov alebo je výkon týchto právomocí vzhľadom na odôvodnenie 11 [rozhodnutia 2010/87] obmedzený iba na výnimočné prípady alebo môže úrad na ochranu údajov využiť svoju voľnú úvahu a neprerušiť toky údajov?

9. a) Predstavuje rozhodnutie [ŠnOOÚ] na účely článku 25 ods. 6 smernice [95/46] všeobecne záväzné konštatovanie, ktoré je záväzné pre úrady na ochranu údajov a súdy členských štátov v zmysle, že USA zabezpečujú primeranú úroveň ochrany v zmysle článku 25 ods. 2 smernice [95/46] z dôvodu svojho vnútroštátneho práva alebo medzinárodných záväzkov, ktoré prijali?
   b) Ak nie, aký (prípadný) význam má rozhodnutie [ŠnOOÚ] pri posudzovaní primeranosti záruk poskytnutých údajom prenášaným do Spojených štátov, ktoré sa prenášajú na základe rozhodnutia [2010/87]?

10. Vzhľadom na zistenia High Court (Vyšší súd) vo vzťahu k právnym predpisom Spojených štátov amerických zabezpečuje inštitút ombudsmana pre štít na ochranu osobných údajov podľa [prílohy A k prílohe III] rozhodnutia [ŠnOOÚ] v spojení s existujúcim režimom v Spojených štátoch prostriedok nápravy pre dotknuté osoby, ktorých osobné údaje sa prenášajú do USA na základe rozhodnutia [2010/87], ktorý je zlučiteľný s článkom 47 Charty?

11. Porušuje rozhodnutie [2010/87] články 7, 8 alebo 47 Charty?“

O prípustnosti návrhu na začatie prejudiciálneho konania

69 Facebook Ireland, ako aj nemecká vláda a vláda Spojeného kráľovstva tvrdia, že návrh na začatie prejudiciálneho konania je neprípustný.

70 Pokiaľ ide o námietku predloženú spoločnosťou Facebook Ireland, táto spoločnosť poznamenáva, že nariadenie GDPR zrušilo ustanovenia smernice 95/46, na ktorých sú založené prejudiciálne otázky.

71 Hoci je v tejto súvislosti pravda, že smernica 95/46 bola v súlade s článkom 94 ods. 1 nariadenia GDPR zrušená s účinnosťou od 25. mája 2018, táto smernica bola účinná ešte 4. mája 2018, keď bol vydaný tento návrh na začatie prejudiciálneho konania, a 9. mája 2018, keď bol doručený Súdnemu dvoru. Okrem toho článok 3 ods. 2 prvá zarážka, články 25 a 26, ako aj článok 28 ods. 3 smernice 95/46, na ktoré odkazujú prejudiciálne otázky, boli v podstate prevzaté do článku 2 ods. 2, ako aj článkov 45, 46 a 58 nariadenia GDPR. Navyše treba pripomenúť, že úlohou Súdneho dvora je vykladať všetky ustanovenia práva Únie, ktoré vnútroštátne súdy potrebujú na rozhodovanie o žalobách, ktoré im boli predložené, aj keď tieto ustanovenia nie sú výslovne spomenuté v otázkach položených Súdnemu dvoru týmito súdmi (rozsudok z 2. apríla 2020, Ruska Federacija, C-897/19 PPU, EU:C:2020:262, bod 43 a citovaná judikatúra). Z týchto rôznych dôvodov okolnosť, že vnútroštátny súd formuloval prejudiciálne otázky s odkazom výlučne na ustanovenia smernice 95/46, nemôže mať za následok neprípustnosť tohto návrhu na začatie prejudiciálneho konania.

72 Nemecká vláda zakladá svoju námietku neprípustnosti jednak na okolnosti, že komisár vyjadril len pochybnosti, a nie konečné stanovisko, pokiaľ ide o otázku platnosti rozhodnutia 2010/87, a jednak na tom, že vnútroštátny súd neoveril, či pán Schrems dal nepochybne svoj súhlas s prenosmi údajov, o ktoré ide vo veci samej, čo by v prípade, že to tak je, spôsobilo, že odpoveď na túto otázku nebude užitočná. Napokon podľa vlády Spojeného kráľovstva majú prejudiciálne otázky hypotetickú povahu, keďže tento súd nekonštatoval, že tieto údaje boli skutočne prenesené na základe uvedeného rozhodnutia.

73 Z ustálenej judikatúry Súdneho dvora vyplýva, že prináleží iba vnútroštátnemu súdu, ktorý prejednáva spor a ktorý nesie zodpovednosť za následné súdne rozhodnutie, aby so zreteľom na osobitosti veci posúdil tak potrebu rozhodnutia v prejudiciálnom konaní na vydanie svojho rozsudku, ako aj relevantnosť otázok, ktoré kladie Súdnemu dvoru. Preto pokiaľ sa predložené otázky týkajú výkladu

právneho predpisu Únie, Súdny dvor je v zásade povinný rozhodnúť. Z toho vyplýva, že pri otázkach položených vnútroštátnymi súdmi platí prezumpcia relevantnosti. Súdny dvor môže odmietnuť návrh na začatie prejudiciálneho konania podaný vnútroštátnym súdom len vtedy, ak sa javí, že požadovaný výklad nemá nijakú súvislosť s existenciou alebo predmetom sporu vo veci samej, ak ide o hypotetický problém alebo ak Súdny dvor nedisponuje skutkovými ani právnymi podkladmi potrebnými na užitočnú odpoveď na uvedené otázky (rozsudky zo 16. júna 2015, Gauweiler a i., C-62/14, EU:C:2015:400, body 24 a 25; z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 45, ako aj z 19. decembra 2019, Dobersberger, C-16/18, EU:C:2019:1110, body 18 a 19).

74 V prejednávanej veci návrh na začatie prejudiciálneho konania obsahuje skutkové a právne okolnosti, ktoré sú dostatočné na pochopenie rozsahu prejudiciálnych otázok. Okrem toho a predovšetkým žiadna skutočnosť v spise, ktorý má Súdny dvor k dispozícii, neumožňuje domnievať sa, že požadovaný výklad práva Únie nemá súvislosť s existenciou alebo predmetom sporu vo veci samej, alebo že ide o hypotetický problém, najmä z dôvodu, že poskytnutie osobných údajov, o ktoré ide vo veci samej, je založené na výslovnom súhlase dotknutej osoby s týmto prenosom, a nie na rozhodnutí 2010/87. Podľa údajov uvedených v tomto návrhu totiž Facebook Ireland uznala, že spoločnosti Facebook Inc. prenáša osobné údaje svojich používateľov s bydliskom v Únii a že veľká časť týchto prenosov, ktorých zákonnosť pán Schrems spochybňuje, sa vykonáva na základe štandardných doložiek o ochrane údajov uvedených v prílohe rozhodnutia 2010/87.

75 Okrem toho na prípustnosť tohto návrhu na začatie prejudiciálneho konania nemá vplyv, že komisár nevyjadril konečné stanovisko k platnosti tohto rozhodnutia, keďže vnútroštátny súd sa domnieva, že odpoveď na prejudiciálne otázky týkajúce sa výkladu a platnosti pravidiel práva Únie je nevyhnutná na vyriešenie sporu vo veci samej.

76 Z toho vyplýva, že návrh na začatie prejudiciálneho konania je prípustný.

O prejudiciálnych otázkach

77 Na úvod treba pripomenúť, že tento návrh na začatie prejudiciálneho konania vychádza zo sťažnosti pána Schremsa, ktorou sa domáha, aby komisár nariadil do budúcnosti pozastaviť alebo zakázať spoločnosti Facebook Ireland prenos jeho osobných údajov spoločnosti Facebook Inc. Keďže prejudiciálne otázky odkazujú na ustanovenia smernice 95/46, je nesporné, že komisár v momente, keď bola táto smernica zrušená a nahradená nariadením GDPR s účinnosťou od 25. mája 2018, ešte neprijal konečné rozhodnutie o tejto sťažnosti.

78 Táto neexistencia vnútroštátneho rozhodnutia odlišuje situáciu vo veci samej od situácií, ktoré viedli k rozsudkom z 24. septembra 2019, Google (Územná pôsobnosť odstránenia odkazu) (C-507/17, EU:C:2019:772), a z 1. októbra 2019, Planet49 (C-673/17, EU:C:2019:801), v ktorých išlo o rozhodnutia prijaté pred zrušením uvedenej smernice.

79 Na prejudiciálne otázky preto treba odpovedať vzhľadom na ustanovenia nariadenia GDPR, a nie na smernicu 95/46.

O prvej otázke

80 Svojou prvou otázkou sa vnútroštátny súd v podstate pýta, či sa článok 2 ods. 1 a článok 2 ods. 2 písm. a), b) a d) nariadenia GDPR v spojení s článkom 4 ods. 2 ZEÚ majú vykladať v tom zmysle, že do pôsobnosti tohto nariadenia patrí prenos osobných údajov vykonaný hospodárskym subjektom usadeným v jednom členskom štáte inému hospodárskemu subjektu usadenému v tretej krajine, ak v priebehu tohto prenosu alebo po ňom môžu byť tieto údaje spracúvané orgánmi tejto tretej krajiny na účely verejnej bezpečnosti, obrany a bezpečnosti štátu.

81 V tejto súvislosti treba na úvod uviesť, že ustanovenie článku 4 ods. 2 ZEÚ, podľa ktorého národná bezpečnosť v rámci Únie ostáva vo výlučnej zodpovednosti každého členského štátu, sa týka výlučne členských štátov Únie. V dôsledku toho toto ustanovenie nie je v prejednávanej veci relevantné pre výklad článku 2 ods. 1 a článku 2 ods. 2 písm. a), b) a d) nariadenia GDPR.

82 Podľa článku 2 ods. 1 nariadenia GDPR sa toto nariadenie vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému. Článok 4 bod 2 tohto nariadenia definuje pojem „spracúvanie“ ako „operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov… automatizovanými alebo neautomatizovanými prostriedkami“, a ako príklad uvádza „poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom“ bez ohľadu na to, či sa tieto operácie vykonávajú v rámci Únie alebo majú spojitosť s treťou krajinou. Okrem toho uvedené nariadenie podriaďuje prenosy osobných údajov do tretích krajín osobitným pravidlám uvedeným v jeho kapitole V, nazvanej „Prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám“, a navyše zveruje dozorným orgánom na tieto účely osobitné právomoci uvedené v článku 58 ods. 2 písm. j) toho istého nariadenia.

83 Z toho vyplýva, že operácia spočívajúca v prenose osobných údajov z členského štátu do tretej krajiny predstavuje sama osebe spracúvanie osobných údajov v zmysle článku 4 bodu 2 nariadenia GDPR vykonané na území členského štátu, na ktoré sa toto nariadenie podľa svojho článku 2 ods. 1 vzťahuje [pozri analogicky, pokiaľ ide o článok 2 písm. b) a článok 3 ods. 1 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 45 a citovanú judikatúru].

84 Pokiaľ ide o otázku, či možno takúto operáciu považovať za vylúčenú z pôsobnosti nariadenia GDPR podľa článku 2 ods. 2 tohto nariadenia, treba pripomenúť, že toto ustanovenie stanovuje výnimky z pôsobnosti tohto nariadenia, ako je vymedzená v jeho článku 2 ods. 1, a že tieto výnimky sa majú vykladať reštriktívne (pozri analogicky, pokiaľ ide o článok 3 ods. 2 smernice 95/46, rozsudok z 10. júla 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, bod 37 a citovanú judikatúru).

85 Keďže v prejednávanej veci sa prenos osobných údajov, o ktorý ide vo veci samej, vykonáva spoločnosťou Facebook Ireland spoločnosti Facebook Inc., teda medzi dvoma právnickými osobami, na tento prenos sa nevzťahuje článok 2 ods. 2 písm. c) nariadenia GDPR, ktorý sa týka spracúvania údajov fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti. Na uvedený prenos sa nevzťahujú ani výnimky uvedené v článku 2 ods. 2 písm. a), b) a d) tohto nariadenia, keďže činnosti demonštratívne uvedené v tomto článku sú v každom prípade činnosti štátu a štátnych orgánov, ktoré nepatria do oblasti činností jednotlivcov (pozri analogicky, pokiaľ ide o článok 3 ods. 2 smernice 95/46, rozsudok z 10. júla 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, bod 38 a citovanú judikatúru).

86 Možnosť, že osobné údaje prenášané medzi dvoma hospodárskymi subjektmi na obchodné účely budú počas prenosu alebo po ňom spracúvané orgánmi dotknutej tretej krajiny na účely verejnej bezpečnosti, obrany a bezpečnosti štátu, nemôže vylúčiť uvedený prenos z pôsobnosti nariadenia GDPR.

87 Okrem toho tým, že sa Komisii výslovne stanovuje povinnosť, aby pri posudzovaní primeranosti úrovne ochrany poskytovanej treťou krajinou zohľadnila najmä „príslušné právne predpisy, a to všeobecné 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“, samotné znenie článku 45 ods. 2 písm. a) tohto nariadenia zdôrazňuje, že prípadné spracúvanie dotknutých osobných údajov treťou krajinou na účely verejnej bezpečnosti, obrany a bezpečnosti štátu nespochybňuje uplatniteľnosť uvedeného nariadenia na predmetný prenos.

88 Z toho vyplýva, že takýto prenos nemôže byť vyňatý z pôsobnosti nariadenia GDPR z dôvodu, že dotknuté údaje môžu v priebehu tohto prenosu alebo po ňom byť spracúvané orgánmi dotknutej tretej krajiny na účely verejnej bezpečnosti, obrany a bezpečnosti štátu.

89 Preto treba na prvú otázku odpovedať tak, že článok 2 ods. 1 a 2 nariadenia GDPR sa má vykladať v tom zmysle, že do pôsobnosti tohto nariadenia patrí prenos osobných údajov vykonaný na obchodné účely hospodárskym subjektom usadeným v jednom členskom štáte inému hospodárskemu subjektu usadenému v tretej krajine bez ohľadu na to, či v priebehu tohto prenosu alebo po ňom môžu byť tieto údaje spracúvané orgánmi dotknutej tretej krajiny na účely verejnej bezpečnosti, obrany a bezpečnosti štátu.

O druhej, tretej a šiestej otázke

90 Svojou druhou, treťou a šiestou otázkou sa vnútroštátny súd Súdneho dvora v podstate pýta na úroveň ochrany vyžadovanú v článku 46 ods. 1 a v článku 46 ods. 2 písm. c) nariadenia GDPR v rámci prenosu osobných údajov do tretej krajiny založeného na štandardných doložkách o ochrane údajov. Tento súd konkrétne žiada Súdny dvor, aby spresnil skutočnosti, ktoré treba zohľadniť na účely určenia, či je táto úroveň ochrany zaručená v kontexte uvedeného prenosu.

91 Pokiaľ ide o požadovanú úroveň ochrany, zo znenia týchto ustanovení v ich vzájomnej spojitosti vyplýva, že v prípade neexistencie rozhodnutia o primeranosti prijatého podľa článku 45 ods. 3 tohto nariadenia môže prevádzkovateľ alebo sprostredkovateľ preniesť osobné údaje do tretej krajiny len vtedy, ak poskytol „primerané záruky“, a pod podmienkou, že dotknuté osoby majú „vymožiteľné práva a účinné právne prostriedky nápravy“, pričom tieto primerané záruky môžu byť poskytnuté najmä prostredníctvom štandardných doložiek o ochrane údajov prijatých Komisiou.

92 Hoci článok 46 nariadenia GDPR nespresňuje povahu požiadaviek, ktoré vyplývajú z tohto odkazu na „primerané záruky“, „vymožiteľné práva“ a „účinné právne prostriedky nápravy“, treba uviesť, že tento článok sa nachádza v kapitole V tohto nariadenia, a preto treba uvedený článok vykladať s ohľadom na článok 44 uvedeného nariadenia, nazvaný „Všeobecná zásada prenosov“, ktorý stanovuje, že „všetky ustanovenia v tejto kapitole sa uplatňujú s cieľom zabezpečiť, aby sa neohrozila úroveň ochrany fyzických osôb zaručená týmto nariadením“. Táto úroveň ochrany musí byť preto zaručená bez ohľadu na ustanovenie uvedenej kapitoly, na základe ktorého sa uskutočňuje prenos osobných údajov do tretej krajiny.

93 Ako totiž uviedol generálny advokát v bode 117 svojich návrhov, cieľom ustanovení kapitoly V nariadenia GDPR je zabezpečiť kontinuitu vysokej úrovne tejto ochrany v prípade prenosu osobných údajov do tretej krajiny v súlade s cieľom uvedeným v odôvodnení 6 tohto nariadenia.

94 Článok 45 ods. 1 prvá veta nariadenia GDPR stanovuje, že prenos osobných údajov do tretej krajiny možno povoliť, ak Komisia prijme rozhodnutie, že táto tretia krajina, územie alebo jeden či viaceré určené sektory v danej krajine zaručujú primeranú úroveň ochrany. V tejto súvislosti sa síce nepožaduje, aby dotknutá tretia krajina zaručila rovnakú úroveň ochrany, ako je úroveň ochrany zaručená v právnom poriadku Únie, výraz „primeraná úroveň ochrany“ treba chápať – ako potvrdzuje odôvodnenie 104 tohto nariadenia – tak, že vyžaduje, aby táto tretia krajina skutočne zabezpečila na základe jej vnútroštátneho práva alebo medzinárodných dohôd úroveň ochrany slobôd a základných práv, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie podľa uvedeného nariadenia v spojení s Chartou. Ak by totiž takáto požiadavka chýbala, cieľ uvedený v predchádzajúcom bode by nebol dodržaný (pozri analogicky, pokiaľ ide o článok 25 ods. 6 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 73).

95 V tejto súvislosti odôvodnenie 107 nariadenia GDPR uvádza, že ak „tretia krajina, územie alebo určený sektor v tretej krajine… už nezaručujú primeranú úroveň ochrany údajov… prenos osobných údajov do tejto tretej krajiny [by sa mal]… zakázať, pokiaľ nie sú splnené požiadavky tohto nariadenia týkajúce sa prenosov na základe primeraných záruk“. Na tento účel odôvodnenie 108 uvedeného nariadenia spresňuje, že v prípade neexistencie rozhodnutia o primeranosti, príslušné záruky, ktoré musí prevádzkovateľ alebo sprostredkovateľ prijať v súlade s článkom 46 ods. 1 toho istého nariadenia, musia

„kompenz[ovať]… nedostatočnú ochranu údajov v tretej krajine“, aby „zabezpeči[li] súlad s požiadavkami na ochranu údajov a právami dotknutých osôb primeranými spracúvaniu v rámci Únie“.

96 Z toho vyplýva, ako uviedol generálny advokát v bode 115 svojich návrhov, že tieto primerané záruky musia byť spôsobilé zabezpečiť, že osobám, ktorých osobné údaje sa prenášajú do tretej krajiny na základe štandardných doložiek o ochrane údajov, prináleží, tak ako pri prenose založenom na rozhodnutí o primeranosti, úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie.

97 Vnútroštátny súd sa tiež pýta, či sa má táto úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie, určiť s ohľadom na právo Únie, najmä práva zaručené Chartou, a/alebo so zreteľom na základné práva zakotvené v Európskom dohovore o ochrane ľudských práv a základných slobôd (ďalej len „EDĽP“) alebo tiež s ohľadom na vnútroštátne právo členských štátov.

98 V tejto súvislosti treba pripomenúť, že ako to potvrdzuje článok 6 ods. 3 ZEÚ, že základné práva zakotvené EDĽP sú súčasťou práva Únie rovnako ako všeobecné zásady, a hoci článok 52 ods. 3 Charty stanovuje, že práva obsiahnuté v Charte, ktoré zodpovedajú právam zaručeným EDĽP, majú rovnaký zmysel a rozsah, ako majú práva priznané uvedeným dohovorom, tento dohovor nepredstavuje, kým k nemu Európska únia nepristúpila, právny nástroj formálne začlenený do právneho poriadku Únie (rozsudky z 26. februára 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, bod 44 a citovaná judikatúra, ako aj z 20. marca 2018, Menci, C-524/15, EU:C:2018:197, bod 22).

99 Za týchto podmienok Súdny dvor rozhodol, že výklad práva Únie, ako aj preskúmanie platnosti aktov Únie musia byť vykonané s ohľadom na základné práva zaručené Chartou (pozri analogicky rozsudok z 20. marca 2018, Menci, C-524/15, EU:C:2018:197, bod 24).

100 Okrem toho z ustálenej judikatúry vyplýva, že platnosť ustanovení práva Únie a pri neexistencii výslovného odkazu na vnútroštátne právo členských štátov výklad týchto ustanovení nemožno posudzovať s ohľadom na uvedené vnútroštátne právo, a to ani ústavnej povahy, konkrétne základné práva, ako sú formulované v ich vnútroštátnej ústave (pozri v tomto zmysle rozsudky zo 17. decembra 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, bod 3; z 13. decembra 1979, Hauer, 44/79, EU:C:1979:290, bod 14, ako aj z 18. októbra 2016, Nikiforidis, C-135/15, EU:C:2016:774, bod 28 a citovanú judikatúru).

101 Z toho vyplýva, že jednak preto, že prenos osobných údajov, o aký ide vo veci samej, ktorý na obchodné účely vykonáva hospodársky subjekt usadený v členskom štáte inému hospodárskemu subjektu usadenému v tretej krajine, patrí, ako vyplýva z odpovede na prvú otázku, do pôsobnosti nariadenia GDPR, a jednak preto, že cieľom tohto nariadenia je, ako vyplýva z jeho odôvodnenia 10, zaručiť konzistentnú a vysokú úroveň ochrany fyzických osôb v rámci Únie a na tento účel zabezpečiť konzistentné a jednotné uplatňovanie pravidiel ochrany základných práv týchto osôb pri spracúvaní osobných údajov v celej Únii, by sa úroveň ochrany základných práv vyžadovaná v článku 46 ods. 1 uvedeného nariadenia mala určiť na základe ustanovení toho istého nariadenia v spojení so základnými právami zaručenými Chartou.

102 Vnútroštátny súd sa snaží ďalej zistiť, aké skutočnosti treba zohľadniť na účely určenia primeranosti úrovne ochrany v kontexte prenosu osobných údajov do tretej krajiny na základe štandardných doložiek o ochrane údajov prijatých podľa článku 46 ods. 2 písm. c) nariadenia GDPR.

103 V tejto súvislosti, hoci toto ustanovenie neuvádza jednotlivé skutočnosti, ktoré treba zohľadniť na účely posúdenia primeranosti úrovne ochrany a ktoré sa majú v rámci takéhoto prenosu dodržiavať, článok 46 ods. 1 tohto nariadenia spresňuje, že dotknuté osoby musia mať k dispozícii primerané záruky, vymožiteľné práva a účinné právne prostriedky nápravy.

104 Posúdenie vyžadované na tento účel v kontexte takéhoto prenosu musí najmä zohľadniť tak zmluvné ustanovenia dohodnuté medzi prevádzkovateľom alebo jeho sprostredkovateľom usadeným v Únii a príjemcom prenosu usadeným v dotknutej tretej krajine, ako aj, pokiaľ ide o prípadný prístup orgánov verejnej moci tejto tretej krajiny k prenášaným osobným údajom, relevantné prvky právneho systému tejto tretej krajiny. V tejto súvislosti skutočnosti, ktoré treba zohľadniť v kontexte článku 46 uvedeného nariadenia, zodpovedajú skutočnostiam, ktoré sú demonštratívne uvedené v článku 45 ods. 2 uvedeného nariadenia.

105 Preto treba na druhú, tretiu a šiestu otázku odpovedať tak, že článok 46 ods. 1 a článok 46 ods. 2 písm. c) nariadenia GDPR sa majú vykladať v tom zmysle, že primerané záruky, vymožiteľné práva a účinné právne prostriedky nápravy vyžadované týmito ustanoveniami musia zabezpečiť, aby práva osôb, ktorých osobné údaje sa prenášajú do tretej krajiny na základe štandardných doložiek o ochrane údajov, požívali úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie týmto nariadením v spojení s Chartou. Na tento účel posúdenie úrovne ochrany zaručenej v kontexte takéhoto prenosu musí najmä zohľadniť tak zmluvné ustanovenia dohodnuté medzi prevádzkovateľom alebo jeho sprostredkovateľom usadeným v Únii a príjemcom prenosu usadeným v dotknutej tretej krajine, ako aj, pokiaľ ide o prípadný prístup orgánov verejnej moci tejto tretej krajiny k takto prenášaným osobným údajom, relevantné prvky právneho systému tejto krajiny, najmä tie, ktoré sú uvedené v článku 45 ods. 2 uvedeného nariadenia.

O ôsmej otázke

106 Svojou ôsmou otázkou sa vnútroštátny súd v podstate pýta, či sa má článok 58 ods. 2 písm. f) a j) nariadenia GDPR vykladať v tom zmysle, že príslušný dozorný orgán je povinný pozastaviť alebo zakázať prenos osobných údajov do tretej krajiny založený na štandardných doložkách o ochrane údajov prijatých Komisiou, ak sa tento dozorný orgán domnieva, že tieto doložky nie sú alebo nemôžu byť v tejto tretej krajine dodržané a že ochrana prenášaných údajov, ktorú vyžaduje právo Únie, najmä články 45 a 46 nariadenia GDPR, ako aj Charta, nemôže byť zaručená, alebo v tom zmysle, že výkon týchto právomocí sa obmedzuje na výnimočné prípady.

107 V súlade s článkom 8 ods. 3 Charty, ako aj článkom 51 ods. 1 a článkom 57 ods. 1 písm. a) nariadenia GDPR sú vnútroštátne dozorné orgány poverené dohľadom nad dodržiavaním pravidiel Únie týkajúcich sa ochrany fyzických osôb pri spracovaní osobných údajov. Každý z nich má preto právomoc overiť, či prenos osobných údajov z členského štátu, ktorému podlieha, do tretej krajiny spĺňa požiadavky stanovené týmto nariadením (pozri analogicky, pokiaľ ide o článok 28 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 47).

108 Z týchto ustanovení vyplýva, že prvoradou úlohou dozorných orgánov je kontrolovať uplatňovanie nariadenia GDPR a dohliadať nad jeho dodržiavaním. Výkon tejto úlohy má osobitný význam v kontexte prenosu osobných údajov do tretej krajiny, keďže ako vyplýva zo samotného znenia odôvodnenia 116 tohto nariadenia „pri cezhraničnom pohybe osobných údajov mimo Úniu môže byť schopnosť fyzických osôb uplatniť si práva na ochranu údajov vystavená vyššiemu riziku, a to najmä pokiaľ ide o ich ochranu pred nezákonným využitím alebo poskytnutím týchto informácií“. V danom prípade, ako bolo spresnené v tomto odôvodnení, „dozorné orgány [môžu] zistiť, že nedokážu vybavovať sťažnosti alebo viesť vyšetrovania týkajúce sa činností vykonávaných za ich hranicami“.

109 Okrem toho podľa článku 57 ods. 1 písm. f) nariadenia GDPR je každý dozorný orgán povinný na svojom území vybavovať sťažnosti, ktoré má v súlade s článkom 77 ods. 1 tohto nariadenia právo podať každá osoba, ak sa domnieva, že spracúvanie osobných údajov, ktoré sa jej týka, je v rozpore s týmto nariadením, a v nevyhnutnom rozsahu preskúmať predmet tejto sťažnosti. Dozorný orgán musí pristúpiť k vybaveniu takejto sťažnosti so všetkou vyžadovanou náležitou starostlivosťou (pozri analogicky, pokiaľ ide o článok 25 ods. 6 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 63).

110 Článok 78 ods. 1 a 2 nariadenia GDPR priznáva každej osobe právo na účinný súdny prostriedok nápravy, najmä ak dozorný orgán sťažnosť nevybavil. Odôvodnenie 141 tohto nariadenia tiež odkazuje na to, že „v súlade s článkom 47 Charty [má] právo na účinný súdny prostriedok nápravy“ v prípade, že tento dozorný orgán „nekoná v prípade, keď je takéto konanie nevyhnutné na ochranu práv dotknutej osoby“.

111 Článok 58 ods. 1 nariadenia GDPR udeľuje na účely vybavovania podaných sťažností každému dozornému orgánu rozsiahle vyšetrovacie právomoci. Ak sa takýto orgán na základe svojho vyšetrovania domnieva, že dotknutá osoba, ktorej osobné údaje boli prenesené do tretej krajiny, nemá v tejto krajine zabezpečenú primeranú úroveň ochrany, je podľa práva Únie povinný reagovať primeraným spôsobom, aby napravil konštatovaný nedostatok, a to bez ohľadu na pôvod alebo povahu tohto nedostatku. Na tento účel článok 58 ods. 2 tohto nariadenia uvádza rôzne nápravné opatrenia, ktoré môže dozorný orgán prijať.

112 Hoci výber vhodného a potrebného prostriedku prináleží dozornému orgánu a tento orgán musí pri tomto výbere zohľadniť všetky okolnosti dotknutého prenosu osobných údajov, nič to nemení na tom, že so všetkou náležitou starostlivosťou je povinný splniť svoju úlohu spočívajúcu v zabezpečení plného dodržiavania nariadenia GDPR.

113 Ako v tejto súvislosti uviedol tiež generálny advokát v bode 148 svojich návrhov, uvedený orgán je na základe článku 58 ods. 2 písm. f) a j) tohto nariadenia povinný pozastaviť alebo zakázať prenos osobných údajov do tretej krajiny, ak sa vzhľadom na všetky osobitné okolnosti tohto prenosu domnieva, že štandardné doložky ochrany údajov nie sú alebo nemôžu byť v tejto tretej krajine dodržané a že ochrana prenášaných údajov, ktorú vyžaduje právo Únie, nemôže byť zabezpečená inými prostriedkami, pokiaľ prevádzkovateľ alebo jeho sprostredkovateľ so sídlom v Únii sám tento prenos nepozastaví alebo neukončí.

114 Výklad uvedený v predchádzajúcom bode nemôže byť vyvrátený argumentáciou komisára, podľa ktorej článok 4 rozhodnutia 2010/87 v znení predchádzajúcom nadobudnutiu účinnosti vykonávacieho rozhodnutia 2016/2297 v spojení s odôvodnením 11 tohto rozhodnutia obmedzoval právomoc dozorných orgánov pozastaviť alebo zakázať prenos osobných údajov do tretej krajiny na určité výnimočné prípady. Článok 4 rozhodnutia 2010/87 totiž vo svojom znení vychádzajúcom z vykonávacieho rozhodnutia 2016/2297 uvádza právomoc, ktorú majú tieto orgány v súčasnosti na základe článku 58 ods. 2 písm. f) a j) nariadenia GDPR, a ktorou je pozastaviť alebo zakázať takýto prenos bez toho, aby sa výkon tejto právomoci akokoľvek obmedzoval na výnimočné okolnosti.

115 V každom prípade vykonávacia právomoc, ktorú článok 46 ods. 2 písm. c) nariadenia GDPR priznáva Komisii na účely prijatia štandardných ustanovení ochrany údajov, jej nepriznáva právomoc obmedziť právomoci, ktoré majú dozorné orgány podľa článku 58 ods. 2 tohto nariadenia (pozri analogicky, pokiaľ ide o článok 25 ods. 6 a článok 28 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, body 102 a 103). Odôvodnenie 5 vykonávacieho rozhodnutia 2016/2297 navyše potvrdzuje, že rozhodnutie 2010/87 „nebráni… dozornému orgánu uplatňovať svoje právomoci pri dohľade nad tokmi údajov vrátane právomoci na pozastavenie alebo zákaz prenosu osobných údajov, keď skonštatuje, že sa prenos uskutočňuje v rozpore s právnymi predpismi [Európskej únie] a vnútroštátnymi právnymi predpismi o ochrane údajov“.

116 Treba však spresniť, že právomoci príslušného dozorného orgánu podliehajú úplnému dodržaniu rozhodnutia, ktorým Komisia na základe článku 45 ods. 1 prvej vety nariadenia GDPR prípadne konštatuje, že určitá tretia krajina zaručuje primeranú úroveň ochrany. V takom prípade totiž z článku 45 ods. 1 druhej vety tohto nariadenia v spojení s jeho odôvodnením 103 vyplýva, že prenosy osobných údajov do dotknutej tretej krajiny sa môže uskutočniť bez toho, aby bolo nutné získať osobitné povolenie.

117 Podľa článku 288 štvrtého odseku ZFEÚ je rozhodnutie Komisie o primeranosti v celom rozsahu záväzné pre všetky členské štáty, ktorým je určené, a teda aj pre všetky ich orgány v rozsahu, v akom konštatuje, že dotknutá tretia krajina zaručuje primeranú úroveň ochrany, a má za následok, že oprávňuje tieto prenosy údajov (pozri analogicky, pokiaľ ide o článok 25 ods. 6 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 51 a citovanú judikatúru).

118 Preto pokiaľ rozhodnutie o primeranosti nebolo Súdnym dvorom vyhlásené za neplatné, členské štáty a ich orgány, medzi ktoré patria ich nezávislé dozorné orgány, nemôžu prijať opatrenia v rozpore s týmto rozhodnutím, akým sú akty, ktorými sa záväzne konštatuje, že tretia krajina dotknutá uvedeným rozhodnutím nezaručuje primeranú úroveň ochrany (rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 52 a citovaná judikatúra), a v dôsledku toho nemôžu pozastaviť alebo zakázať prenosy osobných údajov do tejto tretej krajiny.

119 Rozhodnutie Komisie o primeranosti prijaté na základe článku 45 ods. 3 nariadenia GDPR však nemôže brániť osobám, ktorých osobné údaje boli alebo by mohli byť prenesené do tretej krajiny, obrátiť sa podľa článku 77 ods. 1 nariadenia GDPR na príslušný vnútroštátny dozorný orgán so sťažnosťou týkajúcou sa ochrany ich práv a slobôd v súvislosti so spracúvaním týchto údajov. Rovnako tak rozhodnutie tejto povahy nemôže vylúčiť ani obmedziť právomoci výslovne priznané vnútroštátnym dozorným orgánom podľa článku 8 ods. 3 Charty, ako aj článkom 51 ods. 1 a článkom 57 ods. 1 písm. a) uvedeného nariadenia (pozri analogicky, pokiaľ ide o článok 25 ods. 6 a článok 28 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 53).

120 Teda aj v prípade, že Komisia prijme rozhodnutie o primeranosti, príslušný vnútroštátny dozorný orgán, na ktorý sa osoba obrátila so sťažnosťou týkajúcou sa ochrany jej práv a slobôd v súvislosti so spracovaním osobných údajov, ktoré sa jej týkajú, musí mať možnosť úplne nezávisle preskúmať, či prenos týchto údajov spĺňa požiadavky stanovené nariadením GDPR, a prípadne podať žalobu na vnútroštátne súdy, aby tieto súdy, ak majú rovnaké pochybnosti ako tento orgán, pokiaľ ide o platnosť rozhodnutia o primeranosti, podali návrh na začatie prejudiciálneho konania na účely preskúmania tejto platnosti (pozri analogicky, pokiaľ ide o článok 25 ods. 6 a článok 28 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, body 57 a 65).

121 Vzhľadom na predchádzajúce úvahy treba na ôsmu otázku odpovedať tak, že článok 58 ods. 2 písm. f) a j) nariadenia GDPR sa má vykladať v tom zmysle, že pokiaľ neexistuje rozhodnutie o primeranosti, ktoré Komisia platne prijala, príslušný dozorný orgán je povinný pozastaviť alebo zakázať prenos osobných údajov do tretej krajiny založený na štandardných doložkách o ochrane údajov prijatých Komisiou, ak sa tento dozorný orgán vzhľadom na všetky osobitné okolnosti tohto prenosu domnieva, že tieto doložky nie sú alebo nemôžu byť v tejto tretej krajine dodržané a že ochrana prenášaných údajov, ktorú vyžaduje právo Únie, najmä články 45 a 46 nariadenia GDPR, ako aj Charta, nemôže byť zabezpečená inými prostriedkami, pokiaľ prevádzkovateľ alebo jeho sprostredkovateľ so sídlom v Únii sám tento prenos nepozastaví alebo neukončí.

O siedmej a jedenástej otázke

122 Svojou siedmou a jedenástou otázkou, ktoré treba preskúmať spoločne, sa vnútroštátny súd v podstate pýta Súdneho dvora na platnosť rozhodnutia 2010/87 vzhľadom na články 7, 8 a 47 Charty.

123 Konkrétne, ako vyplýva zo samotného znenia siedmej otázky a súvisiacich vysvetlení uvedených v návrhu na začatie prejudiciálneho konania, vnútroštátny súd sa pýta, či rozhodnutie 2010/87 môže zabezpečiť primeranú úroveň ochrany osobných údajov prenášaných do tretích krajín, vzhľadom na to, že štandardné doložky o ochrane údajov, ktoré stanovuje, nie sú pre orgány týchto tretích krajín záväzné.

124 Článok 1 rozhodnutia 2010/87 stanovuje, že štandardné doložky o ochrane údajov uvedené v prílohe daného rozhodnutia sa považujú za doložky, ktoré poskytujú primerané záruky, pokiaľ ide o ochranu súkromia a základných práv a slobôd jednotlivcov v súlade s požiadavkami článku 26 ods. 2 smernice 95/46. Ustanovenie tohto článku bolo v podstate prevzaté do článku 46 ods. 1 a článku 46 ods. 2 písm. c) GDPR.

125 Hoci tieto doložky sú pre prevádzkovateľa usadeného v Únii a príjemcu prenosu osobných údajov usadeného v tretej krajine, ak uzavreli zmluvu s odkazom na tieto doložky, záväzné, je nesporné, že uvedené doložky nezaväzujú orgány tejto tretej krajiny, pretože nie sú zmluvnými stranami danej zmluvy.

126 Ak teda existujú situácie, keď vzhľadom na právny stav a prax uplatňovanú v dotknutej tretej krajine je príjemca takéhoto prenosu schopný zaručiť vyžadovanú ochranu údajov len na základe štandardných doložiek o ochrane údajov, existujú iné okolnosti, v ktorých ustanovenia obsiahnuté v týchto doložkách nemôžu predstavovať dostatočný prostriedok umožňujúci v praxi zabezpečiť účinnú ochranu osobných údajov prenášaných do dotknutej tretej krajiny. O taký prípad ide najmä vtedy, ak právo tejto tretej krajiny umožňuje jej orgánom verejnej moci zasahovať do práv dotknutých osôb týkajúcich sa týchto údajov.

127 Vzniká teda otázka, či je rozhodnutie Komisie týkajúce sa štandardných doložiek o ochrane údajov, ktoré bolo prijaté na základe článku 46 ods. 2 písm. c) nariadenia GDPR, neplatné, keďže v tomto rozhodnutí neexistujú záruky uplatniteľné voči orgánom verejnej moci tretích krajín, do ktorých sú alebo by mohli byť osobné údaje na základe týchto doložiek prenášané.

128 Článok 46 ods. 1 GDPR stanovuje, že v prípade neexistencie rozhodnutia o primeranosti môže prevádzkovateľ alebo sprostredkovateľ uskutočniť prenos osobných údajov do tretej krajiny len vtedy, ak poskytol primerané záruky, a pod podmienkou, že dotknuté osoby majú k dispozícii vymožiteľné práva a účinné právne prostriedky nápravy. Podľa článku 46 ods. 2 písm. c) tohto nariadenia môžu byť tieto záruky poskytnuté prostredníctvom štandardných doložiek o ochrane údajov prijatých Komisiou. Tieto ustanovenia však neuvádzajú, že všetky uvedené záruky musia byť nevyhnutne stanovené rozhodnutím Komisie, akým je rozhodnutie 2010/87.

129 V tejto súvislosti treba uviesť, že takéto rozhodnutie sa odlišuje od rozhodnutia o primeranosti prijatého na základe článku 45 ods. 3 nariadenia GDPR, ktorého cieľom je v dôsledku preskúmania právnej úpravy dotknutej tretej krajiny, a najmä s prihliadnutím na relevantnú právnu úpravu v oblasti národnej bezpečnosti a prístupu orgánov verejnej moci k osobným údajom konštatovať so záväzným účinkom, že tretia krajina, územie alebo jeden či viaceré určené sektory v danej krajine zaručujú primeranú úroveň ochrany, a teda že prístup orgánov verejnej moci danej tretej krajiny nebráni prenosom údajov do tejto tretej krajiny. Takéto rozhodnutie o primeranosti môže Komisia prijať len pod podmienkou, že dospela k záveru, že relevantná právna úprava tejto tretej krajiny skutočne obsahuje všetky požadované záruky, na základe ktorých sa môže domnievať, že zaručuje primeranú úroveň ochrany.

130 Naopak, pokiaľ ide o rozhodnutie Komisie, ktorým sa prijímajú štandardné doložky o ochrane údajov, akým je rozhodnutie 2010/87, keďže sa takéto rozhodnutie netýka tretej krajiny, územia alebo jedného či viacerých určených sektorov v danej krajine, z článku 46 ods. 1 a článku 46 ods. 2 písm. c) nariadenia GDPR nemožno vyvodiť, že Komisia bola povinná pred prijatím takéhoto rozhodnutia vykonať posúdenie primeranosti úrovne ochrany zabezpečovanej tretími krajinami, do ktorých mohli byť také osobné údaje na základe takých doložiek prenesené.

131 V tejto súvislosti treba pripomenúť, že podľa článku 46 ods. 1 tohto nariadenia v prípade, že Komisia nerozhodne o primeranosti, je úlohou najmä prevádzkovateľa alebo sprostredkovateľa, ktorí sú usadení v Únii, aby poskytli primerané záruky. Odôvodnenia 108 a 114 uvedeného nariadenia potvrdzujú, že keď sa Komisia nevyjadrila k primeranosti úrovne ochrany údajov v tretej krajine, prevádzkovateľ

alebo prípadne jeho sprostredkovateľ by „mali prijať opatrenia na kompenzáciu za nedostatočnú ochranu údajov v tretej krajine prostredníctvom primeraných záruk pre dotknutú osobu“ a že „tieto záruky by mali zabezpečiť súlad s požiadavkami na ochranu údajov a právami dotknutých osôb primeranými spracúvaniu v rámci Únie vrátane dostupnosti vymáhateľných práv dotknutých osôb a účinných právnych prostriedkov nápravy… v Únii alebo tretej krajine“.

132 Keďže, ako vyplýva z bodu 125 tohto rozsudku, zo zmluvnej povahy štandardných doložiek o ochrane údajov vyplýva, že tieto doložky nemôžu zaväzovať orgány verejnej moci tretích krajín, ale že článok 44, článok 46 ods. 1 a článok 46 ods. 2 písm. c) nariadenia GDPR vykladané s prihliadnutím na články 7, 8 a 47 Charty vyžadujú, aby nebola ohrozená úroveň ochrany fyzických osôb zaručená týmto nariadením, môže sa ukázať ako nevyhnutné doplniť záruky, ktoré obsahujú tieto štandardné doložky o ochrane údajov. V tejto súvislosti odôvodnenie 109 daného nariadenia uvádza, že „možnosť pre prevádzkovateľa… uplatniť štandardné doložky o ochrane údajov prijaté Komisiou… by nemali [prevádzkovateľom] brániť v tom, aby… k nim pridali ďalšie doložky alebo dodatočné záruky“ a konkrétne spresňuje, že „by sa mali nabádať, aby poskytovali dodatočné záruky…, ktoré doplnia štandardné ochranné doložky [údajov]“.

133 Zdá sa teda, že cieľom štandardných doložiek o ochrane údajov prijatých Komisiou na základe článku 46 ods. 2 písm. c) toho istého nariadenia je výlučne poskytnúť prevádzkovateľom alebo ich sprostredkovateľom usadeným v Únii zmluvné záruky, ktoré sa uplatňujú jednotne vo všetkých tretích krajinách, a teda nezávisle od úrovne ochrany zaručenej v každej z nich. Keďže tieto štandardné doložky o ochrane údajov nemôžu vzhľadom na svoju povahu poskytnúť záruky nad rámec zmluvnej povinnosti, ktoré by dbali na to, aby úroveň ochrany vyžadovaná právom Únie bola dodržaná, môžu však vyžadovať v závislosti od situácie existujúcej v určitej tretej krajine, aby prevádzkovateľ prijal dodatočné opatrenia s cieľom zaručiť dodržiavanie tejto úrovne ochrany.

134 V tejto súvislosti, ako uviedol generálny advokát v bode 126 svojich návrhov, zmluvný mechanizmus stanovený v článku 46 ods. 2 písm. c) nariadenia GDPR je založený na vyvodení zodpovednosti voči prevádzkovateľovi alebo jeho sprostredkovateľovi usadeným v Únii, ako aj subsidiárne tiež voči príslušným dozorným orgánom. Prináleží teda predovšetkým tomuto prevádzkovateľovi alebo jeho sprostredkovateľovi, aby v každom jednotlivom prípade a eventuálne v spolupráci s príjemcom prenosu overil, či právo tretej krajiny určenia zaručuje primeranú ochranu osobných údajov prenášaných na základe štandardných doložiek o ochrane údajov z hľadiska práva Únie a v prípade potreby poskytol dodatočné záruky k zárukám poskytovaným týmito ustanoveniami.

135 Ak prevádzkovateľ alebo jeho sprostredkovateľ usadení v Únii nemôžu prijať dostatočné dodatočné opatrenia na zabezpečenie takejto ochrany, tieto osoby alebo subsidiárne príslušný dozorný orgán musia pozastaviť alebo ukončiť prenos osobných údajov do dotknutej tretej krajiny. Je to tak najmä v prípade, ak právo tejto tretej krajiny ukladá príjemcovi prenosu osobných údajov pochádzajúcich z Únie povinnosti, ktoré sú v rozpore s uvedenými doložkami, a teda také, ktoré môžu spochybniť zmluvnú záruku primeranej úrovne ochrany pred prístupom orgánov verejnej moci uvedenej tretej krajiny k týmto údajom.

136 Preto samotná skutočnosť, že štandardné doložky o ochrane údajov uvedené v rozhodnutí Komisie prijatom na základe článku 46 ods. 2 písm. c) nariadenia GDPR, ako sú doložky uvedené v prílohe rozhodnutia 2010/87, nezaväzujú orgány tretích krajín, do ktorých môžu byť osobné údaje prenesené, nemôže mať vplyv na platnosť tohto rozhodnutia.

137 Táto platnosť naopak závisí od toho, či v súlade s požiadavkou vyplývajúcou z článku 46 ods. 1 a článku 46 ods. 2 písm. c) nariadenia GDPR, vykladaných s prihliadnutím na články 7, 8 a 47 Charty, takéto rozhodnutie obsahuje účinné mechanizmy, ktoré v praxi umožňujú zabezpečiť, aby bola dodržaná úroveň ochrany vyžadovaná právom Únie a aby sa prenosy osobných údajov založené na takýchto doložkách v prípade ich porušenia alebo nemožnosti ich dodržať pozastavili alebo zakázali.

138 Pokiaľ ide o záruky obsiahnuté v štandardných doložkách o ochrane údajov uvedených v prílohe rozhodnutia 2010/87, z doložky 4 písm. a) a b), doložky 5 písm. a), doložky 9, ako aj doložky 11 ods. 1 tejto prílohy vyplýva, že prevádzkovateľ usadený v Únii, príjemca prenosu osobných údajov, ako aj prípadný sprostredkovateľ tohto prenosu sa vzájomne zaväzujú, že spracovanie týchto údajov vrátane ich prenosu bolo, a naďalej bude uskutočňované v súlade s „príslušn[ým] právo[m] týkajúc[im] sa ochrany údajov“, t. j. podľa definície uvedenej v článku 3 písm. f) uvedeného rozhodnutia, v súlade s „právn[ymi] predpis[mi] chrániac[imi] základné práva a slobody jednotlivcov a najmä ich právo [na súkromie] vo vzťahu k spracovaniu osobných údajov, uplatniteľn[ými] na prevádzkovateľa údajov v členskom štáte, v ktorom je vývozca údajov usadený“. Ustanovenia nariadenia GDPR v spojení s Chartou sú súčasťou týchto právnych predpisov.

139 Okrem toho príjemca prenosu osobných údajov usadený v tretej krajine sa na základe tejto doložky 5 písm. a) zaväzuje bezodkladne informovať prevádzkovateľa usadeného v Únii o jeho prípadnej nemožnosti dodržiavať povinnosti, ktoré mu vyplývajú z uzavretej zmluvy. Konkrétne podľa uvedenej doložky 5 písm. b) tento príjemca potvrdzuje, že nemá dôvod sa domnievať, že právne predpisy, ktorým podlieha, mu bránia plniť záväzky vyplývajúce z uzavretej zmluvy, a zaväzuje sa oznámiť prevádzkovateľovi bezodkladne po tom, ako sa o zmene právnych predpisov dozvedel, každú ich zmenu, ktorá by mohla mať závažný nepriaznivý účinok na záruky a záväzky stanovené štandardnými doložkami o ochrane údajov, ktoré sú uvedené v prílohe rozhodnutia 2010/87. Okrem toho, hoci samotná doložka 5 písm. d) bod i) umožňuje príjemcovi prenosu osobných údajov v prípade právnych predpisov, ktoré takýto postup odôvodňujú, akým je zákaz trestnoprávnej povahy v záujme zachovania dôvernosti vyšetrovania v rámci presadzovania práva, neoznámiť prevádzkovateľovi usadenému v Únii, že orgán presadzovania práva podal právne záväznú žiadosť na sprístupnenie osobných údajov, v súlade s doložkou 5 písm. a) prílohy rozhodnutia 2010/87 je prinajmenšom povinný prevádzkovateľa informovať, že nemôže zabezpečiť dodržiavanie štandardných doložiek o ochrane údajov.

140 V oboch prípadoch, ktoré táto doložka 5 písm. a) a b) upravuje, priznáva prevádzkovateľovi usadenému v Únii právo pozastaviť prenos údajov a/alebo vypovedať zmluvu. Vzhľadom na požiadavky vyplývajúce z článku 46 ods. 1 a článku 46 ods. 2 písm. c) nariadenia GDPR v spojení s článkami 7 a 8 Charty pozastavenie prenosu údajov a/alebo vypovedanie zmluvy sú pre prevádzkovateľa povinné, ak prijímateľ prenosu nie je alebo už nie je schopný dodržať štandardné doložky o ochrane údajov. V opačnom prípade by prevádzkovateľ porušil požiadavky, ktoré mu vyplývajú z doložky 4 písm. a) prílohy rozhodnutia 2010/87 vykladanej s prihliadnutím na ustanovenia nariadenia GDPR a Charty.

141 Zdá sa teda, že doložka 4 písm. a) doložka 5 písm. a) a b) tejto prílohy ukladajú prevádzkovateľovi usadenému v Únii a príjemcovi prenosu osobných údajov povinnosť zabezpečiť, aby právna úprava tretej krajiny určenia umožnila uvedenému príjemcovi dodržať štandardné doložky o ochrane údajov uvedené v prílohe rozhodnutia 2010/87 predtým, ako pristúpi k prenosu osobných údajov do tejto tretej krajiny. Pokiaľ ide o toto overenie, poznámka pod čiarou týkajúca sa doložky 5 spresňuje, že povinné požiadavky týchto právnych predpisov, ktoré nepresahujú rámec toho, čo je v demokratickej spoločnosti nevyhnutné na zabezpečenie osobitne bezpečnosti štátu, obrany a verejnej bezpečnosti, nie sú v rozpore so štandardnými doložkami o ochrane údajov. Naopak, ako zdôraznil generálny advokát v bode 131 svojich návrhov, splnenie si povinnosti uloženej právom tretej krajiny určenia, ktorá ide nad rámec toho, čo je na tento účel nevyhnutné, treba považovať za porušenie uvedených doložiek. Posúdenie nevyhnutnosti takejto povinnosti uvedenými hospodárskymi subjektmi musí v prípade potreby zohľadniť zistenie o primeranosti úrovne ochrany zabezpečovanej dotknutou treťou krajinou, ktoré je uvedené v rozhodnutí Komisie o primeranosti prijatého na základe článku 45 ods. 3 nariadenia GDPR.

142 Z toho vyplýva, že prevádzkovateľ usadený v Únii a príjemca prenosu osobných údajov sú povinní vopred overiť, či sa v dotknutej tretej krajine dodržiava úroveň ochrany vyžadovaná právom Únie. Príjemca tohto prenosu je v prípade potreby podľa tejto istej doložky 5 písm. b) povinný informovať prevádzkovateľa o jeho prípadnej nemožnosti zabezpečiť dodržanie týchto podmienok, pričom povinnosťou tohto prevádzkovateľa je vtedy pozastaviť prenos údajov a/alebo vypovedať zmluvu.

143 Ak príjemca prenosu osobných údajov do tretej krajiny oznámil prevádzkovateľovi na základe doložky 5 písm. b) prílohy rozhodnutia 2010/87, že právna úprava dotknutej tretej krajiny mu neumožňuje zabezpečiť dodržanie štandardných doložiek o ochrane údajov uvedených v tejto prílohe, z doložky 12 uvedenej prílohy vyplýva, že údaje, ktoré už boli prenesené do tejto tretej krajiny, a ich kópie musia byť v celom rozsahu vrátené alebo zničené. V každom prípade doložka 6 tej istej prílohy sankcionuje porušenie týchto štandardných doložiek tým, že priznáva dotknutej osobe právo na náhradu spôsobenej škody.

144 Treba dodať, že podľa doložky 4 písm. f) prílohy rozhodnutia 2010/87 sa prevádzkovateľ usadený v Únii zaväzuje, že subjekt údajov bude pred prenosom údajov alebo čo najskôr po ňom informovaný o tom, ak by prenos zahŕňal osobitné kategórie údajov, ktoré by mohli byť prenesené do tretej krajiny, ktorá neposkytuje primeranú úroveň ochrany. Táto informácia môže umožniť danej osobe uplatniť právo podať opravný prostriedok, ktoré jej priznáva doložka 3 ods. 1, proti prevádzkovateľovi, aby tento prevádzkovateľ pozastavil plánovaný prenos, odstúpil od zmluvy uzavretej s príjemcom prenosu osobných údajov alebo prípadne požiadal tohto príjemcu o vrátenie alebo zničenie prenesených údajov.

145 Napokon podľa doložky 4 písm. g) uvedenej prílohy prevádzkovateľ usadený v Únii je v prípade, keď mu príjemca prenosu osobných údajov na základe doložky 5 písm. b) tejto prílohy oznámi, že právna úprava, ktorá sa ho týka, je predmetom zmeny, ktorá môže mať závažné nepriaznivé účinky na záruky a záväzky stanovené štandardnými doložkami o ochrane údajov, povinný postúpiť toto oznámenie príslušnému dozornému orgánu, pokiaľ sa vývozca údajov napriek uvedenému oznámeniu rozhodne pokračovať v prenose alebo zrušiť jeho pozastavenie. Na základe predloženia takéhoto oznámenia tomuto dozornému orgánu a vzhľadom na jeho právo vykonať overenia u príjemcu prenosu osobných údajov podľa doložky 8 ods. 2 tej istej prílohy môže uvedený orgán overiť, či treba pristúpiť k pozastaveniu alebo zákazu zamýšľaného prenosu s cieľom zaručiť primeranú úroveň ochrany.

146 V tomto kontexte článok 4 rozhodnutia 2010/87 v spojení s odôvodnením 5 vykonávacieho rozhodnutia 2016/2297 potvrdzuje, že rozhodnutie 2010/87 nijako nebráni príslušnému dozornému orgánu pozastaviť alebo prípadne zakázať prenos osobných údajov do tretej krajiny založený na štandardných doložkách o ochrane údajov uvedených v prílohe k tomuto rozhodnutiu. V tejto súvislosti, ako vyplýva z odpovede na ôsmu otázku, že pokiaľ neexistuje rozhodnutie o primeranosti, ktoré Komisia platne prijala, príslušný dozorný orgán je na základe článku 58 ods. 2 písm. f) a j) nariadenia GDPR povinný pozastaviť alebo zakázať taký prenos, ak sa vzhľadom na všetky osobitné okolnosti tohto prenosu domnieva, že tieto doložky nie sú alebo nemôžu byť v tejto tretej krajine dodržané a že ochrana prenesených údajov vyžadovaná podľa práva Únie nemôže byť zabezpečená inými prostriedkami, pokiaľ prevádzkovateľ alebo jeho sprostredkovateľ so sídlom v Únii sám tento prenos nepozastaví alebo neukončí.

147 Pokiaľ ide o okolnosť zdôraznenú komisárom, že prenosy osobných údajov do takejto tretej krajiny by prípadne mohli byť predmetom rozdielnych rozhodnutí dozorných orgánov v rôznych členských štátoch, treba dodať, že z článku 55 ods. 1 a článku 57 ods. 1 písm. a) nariadenia GDPR vyplýva, že úloha zabezpečiť dodržiavanie tohto nariadenia je v zásade zverená každému dozornému orgánu na území jeho členského štátu. Okrem toho článok 64 ods. 2 uvedeného nariadenia s cieľom predísť rozdielnym rozhodnutiam stanovuje možnosť pre dozorný orgán, ktorý sa domnieva, že prenosy údajov do tretej krajiny musia byť vo všeobecnosti zakázané, požiadať o stanovisko Európsky výbor pre ochranu údajov (EDPB), ktorý môže na základe článku 65 ods. 1 písm. c) toho istého nariadenia prijať záväzné rozhodnutie, najmä ak dozorný orgán nepostupuje podľa vydaného stanoviska.

148 Z toho vyplýva, že rozhodnutie 2010/87 stanovuje účinné mechanizmy, ktoré v praxi umožňujú zabezpečiť, že prenos osobných údajov do tretej krajiny na základe štandardných doložiek o ochrane údajov uvedených v prílohe tohto rozhodnutia bude pozastavený alebo zakázaný, ak príjemca prenosu nedodržiava uvedené doložky alebo nie je schopný ich dodržiavať.

149 Vzhľadom na všetky predchádzajúce úvahy treba na siedmu a jedenástu otázku odpovedať tak, že preskúmanie rozhodnutia 2010/87 vzhľadom na články 7, 8 a 47 Charty neodhalilo nijakú skutočnosť, ktorá by mohla ovplyvniť platnosť tohto rozhodnutia.

O štvrtej, piatej, deviatej a desiatej otázke

150 Svojou deviatou otázkou sa vnútroštátny súd snaží v podstate zistiť, či a v akom rozsahu je dozorný orgán členského štátu viazaný zisteniami uvedenými v rozhodnutí ŠnOOÚ, podľa ktorých Spojené štáty zabezpečujú primeranú úroveň ochrany. Svojou štvrtou, piatou a desiatou otázkou sa tento súd v podstate pýta, či vzhľadom na jeho vlastné zistenia týkajúce sa práva Spojených štátov, prenos osobných údajov do tejto tretej krajiny na základe štandardných doložiek o ochrane údajov uvedených v prílohe rozhodnutia 2010/87 porušuje práva zaručené v článkoch 7, 8 a 47 Charty a Súdneho dvora sa pýta najmä na to, či je zriadenie ombudsmana uvedené v prílohe III rozhodnutia o ŠnOOÚ zlučiteľné s týmto článkom 47.

151 Na úvod treba uviesť, že hoci žaloba vo veci samej, ktorú podal komisár, spochybňuje platnosť len rozhodnutia 2010/87, táto žaloba bola podaná na vnútroštátny súd pred prijatím rozhodnutia ŠnOOÚ. Keďže tento súd sa svojou štvrtou a piatou otázkou vo všeobecnosti pýta Súdneho dvora na ochranu, ktorá sa má podľa článkov 7, 8 a 47 Charty zabezpečiť s ohľadom na takýto prenos, preskúmanie Súdneho dvora musí zohľadniť dôsledky vyplývajúce z rozhodnutia ŠnOOÚ, ktoré bolo medzitým prijaté. Platí to o to viac, ako sa uvedený súd svojou desiatou otázkou výslovne pýta, ak je ochrana požadovaná týmto článkom 47 zabezpečená prostredníctvom ombudsmana uvedeného v uvedenom rozhodnutí.

152 Okrem toho z informácií uvedených v návrhu na začatie prejudiciálneho konania vyplýva, že v rámci konania vo veci samej Facebook Ireland tvrdila, že rozhodnutie ŠnOOÚ malo pre komisára záväzné účinky, pokiaľ ide o zistenie primeranosti úrovne ochrany zabezpečenej Spojenými štátmi, a v dôsledku toho, pokiaľ ide o zákonnosť prenosu osobných údajov do tejto tretej krajiny, ktorý sa zakladá na štandardných doložkách o ochrane údajov uvedených v prílohe rozhodnutia 2010/87.

153 Ako však vyplýva z bodu 59 tohto rozsudku, vnútroštátny súd vo svojom rozsudku z 3. októbra 2017, pripojenom k návrhu na začatie prejudiciálneho konania zdôraznil, že bol povinný zohľadniť zmeny práva, ku ktorým došlo medzi podaním žaloby a pojednávaním, ktoré sa pred ním uskutočnilo. Tento súd je teda údajne na účely rozhodnutia sporu vo veci samej povinný zohľadniť zmenu okolností vyplývajúcich z prijatia rozhodnutia ŠnOOÚ, ako aj prípadné záväzné účinky tohto rozhodnutia.

154 Konkrétne existencia záväzných účinkov, ktoré sa viažu na zistenia uvedené v rozhodnutí ŠnOOÚ o primeranej úrovni ochrany v Spojených štátoch, je relevantná na účely posúdenia tak povinností pripomenutých v bodoch 141 a 142 tohto rozsudku, ktoré prináležia prevádzkovateľovi a príjemcovi prenosu osobných údajov prenášaných do tretej krajiny na základe štandardných doložiek o ochrane údajov uvedených v prílohe rozhodnutia 2010/87, ako aj povinností, ktoré prípadne prináležia dozornému orgánu takýto prenos pozastaviť alebo zakázať.

155 Pokiaľ totiž ide o záväzné účinky rozhodnutia ŠnOOÚ, článok 1 ods. 1 tohto rozhodnutia stanovuje, že na účely článku 45 ods. 1 nariadenia GDPR „Spojené štáty zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám v USA v rámci štítu na ochranu osobných údajov medzi [Európskou úniou] a USA“. V súlade s článkom 1 ods. 3 uvedeného rozhodnutia sa osobné údaje považujú za prenášané v rámci tohto štítu, ak sa prenášajú z Únie organizáciám usadeným v Spojených štátoch, zahrnutým do zoznamu organizácií zapojených do uvedeného štítu, ktorý vedie a sprístupňuje verejnosti Ministerstvo obchodu USA v súlade s oddielmi I a III zásad stanovených v prílohe II toho istého rozhodnutia.

156 Ako vyplýva z judikatúry pripomenutej v bodoch 117 a 118 tohto rozsudku, rozhodnutie ŠnOOÚ je pre dozorné orgány záväzné v rozsahu, v akom konštatuje, že Spojené štáty zaručujú primeranú úroveň ochrany, a teda jeho účinkom je povoliť prenosy osobných údajov uskutočňované v rámci štítu na ochranu osobných údajov medzi Európskou úniou a USA. Preto pokiaľ Súdny dvor toto rozhodnutie nevyhlási za neplatné, príslušný dozorný orgán nemôže pozastaviť alebo zakázať prenos osobných údajov organizácii zapojenej do tohto štítu z dôvodu, že na rozdiel od posúdenia vykonaného Komisiou v uvedenom rozhodnutí sa domnieva, že právna úprava Spojených štátov, ktorá upravuje prístup k osobným údajom prenášaným v rámci uvedeného štítu a používanie týchto údajov orgánmi verejnej moci tejto tretej krajiny na účely národnej bezpečnosti, dodržiavania zákona alebo verejného záujmu nezabezpečuje primeranú úroveň ochrany.

157 Nič to však nemení na tom, že v súlade s judikatúrou pripomenutou v bodoch 119 a 120 tohto rozsudku, keď sa osoba obráti na príslušný dozorný orgán so sťažnosťou, príslušný dozorný orgán musí úplne nezávisle preskúmať, či predmetný prenos osobných údajov spĺňa požiadavky stanovené nariadením GDPR, a v prípade, že považuje výhrady uvedené touto osobou na účely spochybnenia platnosti rozhodnutia o primeranosti za dôvodné, musí podať žalobu na vnútroštátne súdy, aby sa mohli obrátiť na Súdny dvor s návrhom na začatie prejudiciálneho konania týkajúcim sa platnosti tohto rozhodnutia.

158 Sťažnosť podaná podľa článku 77 ods. 1 nariadenia GDPR, ktorou osoba, ktorej osobné údaje boli alebo by mohli byť prenesené do tretej krajiny, uvádza, že právo a prax tejto krajiny nezaisťujú, napriek tomu, čo konštatovala Komisia v rozhodnutí prijatom podľa článku 45 ods. 3 tohto nariadenia, primeranú úroveň ochrany, treba totiž vnímať v podstate ako vzťahujúcu sa na zlučiteľnosť tohto rozhodnutia s ochranou súkromia, ako aj slobôd a základných práv osôb (pozri analogicky, pokiaľ ide o článok 25 ods. 6 a článok 28 ods. 4 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 59).

159 V prejednávanej veci pán Schrems v podstate požiadal komisára, aby zakázal alebo pozastavil prenos osobných údajov vykonávaný spoločnosťou Facebook Ireland na spoločnosť Facebook Inc. usadenú v Spojených štátoch, z dôvodu, že táto tretia krajina nezaručuje primeranú úroveň ochrany. Keďže komisár sa po preskúmaní tvrdení pána Schremsa obrátil na vnútroštátny súd, tento súd sa vzhľadom na predložené dôkazy a kontradiktórnu debatu pred ním zrejme pýta na dôvodnosť pochybností pána Schremsa, pokiaľ ide o primeranosť úrovne ochrany zaručenej v danej tretej krajine, a to napriek tomu, čo Komisia medzitým konštatovala v rozhodnutí ŠnOOÚ, čo viedlo tento súd k položeniu štvrtej, piatej a desiatej prejudiciálnej otázky Súdnemu dvoru.

160 Ako uviedol generálny advokát v bode 175 svojich návrhov, tieto prejudiciálne otázky treba chápať tak, že sa nimi v podstate spochybňuje zistenie Komisie uvedené v rozhodnutí ŠnOOÚ, že Spojené štáty zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie do tejto tretej krajiny, a teda sa nimi spochybňuje aj platnosť tohto rozhodnutia.

161 Vzhľadom na skutočnosti uvedené v bodoch 121 a 157 až 160 tohto rozsudku a s cieľom poskytnúť úplnú odpoveď vnútroštátnemu súdu treba teda preskúmať, či rozhodnutie ŠnOOÚ spĺňa požiadavky vyplývajúce z nariadenia GDPR vykladené v spojení s Chartou (pozri analogicky rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 67).

162 Prijatie rozhodnutia o primeranosti podľa článku 45 ods. 3 nariadenia GDPR Komisiou vyžaduje riadne odôvodnené konštatovanie tejto inštitúcie, že dotknutá tretia krajina z dôvodu jej vnútroštátneho práva alebo medzinárodných dohôd skutočne zabezpečuje úroveň ochrany základných práv, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v právnom poriadku Únie (pozri analogicky, pokiaľ ide o článok 25 ods. 6 smernice 95/46, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 96).

O obsahu rozhodnutia ŠnOOÚ

163 Komisia v článku 1 ods. 1 rozhodnutia ŠnOOÚ konštatovala, že Spojené štáty zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám usadeným v Spojených štátoch v rámci štítu na ochranu údajov medzi Európskou úniou a USA, ktorý podľa článku 1 ods. 2 tohto rozhodnutia tvoria najmä zásady vydané americkým ministerstvom obchodu 7. júla 2016, ktoré sú uvedené v prílohe II uvedeného rozhodnutia, ako aj záväzky obsiahnuté v dokumentoch uvedených v prílohách I, III až VII toho istého rozhodnutia.

164 Rozhodnutie ŠnOOÚ v bode I.5 prílohy II, nazvanej „Zásady rámca štítu na ochranu osobných údajov medzi [Európskou úniou] a USA vydané ministerstvom obchodu USA“, však tiež spresňuje, že dodržiavanie zásad môže byť obmedzené najmä „požiadavk[ami] národnej bezpečnosti, verejného záujmu [a] presadzovania práva“. Toto rozhodnutie tak rovnako ako rozhodnutie 2000/520 zakotvuje prednosť týchto požiadaviek pred uvedenými zásadami, na základe ktorej americké samocertifikované organizácie, ktoré získali osobné údaje z Únie, sú povinné bez akéhokoľvek obmedzenia neuplatniť tieto zásady, ak sú v rozpore s týmito požiadavkami, a teda sú s nimi nezlučiteľné (pozri analogicky, pokiaľ ide o rozhodnutie 2000/520, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 86).

165 Vzhľadom na všeobecnú povahu výnimky uvedenej v bode I.5 prílohy II rozhodnutia ŠnOOÚ táto výnimka umožňuje zasahovanie založené na požiadavkách týkajúcich sa národnej bezpečnosti, verejného záujmu alebo vnútroštátneho práva Spojených štátov, a to do základných práv osôb, ktorých osobné údaje sú alebo by mohli byť prenesené z Únie do Spojených štátov (pozri analogicky, pokiaľ ide o rozhodnutie 2000/520, rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 87). Presnejšie a ako bolo konštatované v rozhodnutí ŠnOOÚ, takéto zásahy môžu vyplývať z prístupu k osobným údajom prenášaným z Únie do Spojených štátov a z použitia týchto údajov americkými orgánmi verejnej moci v rámci programov sledovania PRISM a UPSTREAM založených na článku 702 FISA, ako aj na základe E.O. 12333.

166 V tejto súvislosti Komisia v odôvodneniach 67 až 135 rozhodnutia ŠnOOÚ posúdila obmedzenia a záruky stanovené v právnej úprave Spojených štátov, najmä v článku 702 FISA, E.O. 12333 a PPD-28, týkajúce sa prístupu k osobným údajom, ktoré sú prenášané v rámci štítu na ochranu osobných údajov medzi Európskou úniou a USA, a ich používaním orgánmi verejnej moci Spojených štátov na účely národnej bezpečnosti, presadzovania práva a iné účely všeobecného záujmu.

167 Na základe tohto posúdenia Komisia v odôvodnení 136 tohto rozhodnutia konštatovala, že „USA zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám v USA, ktoré osvedčili svoje dodržiavanie zásad“, a v odôvodnení 140 uvedeného rozhodnutia uviedla, že „na základe dostupných informácií o právnom poriadku USA vrátane vyhlásení a záväzkov vlády USA… akékoľvek zásahy orgánov verejnej moci USA do základných práv osôb, ktorých údaje sa prenášajú z Únie do USA v rámci štítu na ochranu osobných údajov na účely národnej bezpečnosti, presadzovania práva alebo iných verejných záujmov, a následné obmedzenia organizácií, ktoré osvedčili svoje dodržiavanie zásad, s ohľadom na to, ako dodržiavajú zásady, budú obmedzené na to, čo je nevyhnutne potrebné na dosiahnutie príslušného legitímneho cieľa, a že existuje účinná právna ochrana pred takými zásahmi“.

O konštatovaní týkajúcom sa primeranej úrovne ochrany

168 Vzhľadom na skutočnosti uvedené Komisiou v rozhodnutí ŠnOOÚ, ako aj na skutočnosti, ktoré zistil vnútroštátny súd v rámci konania vo veci samej, má tento súd pochybnosti o tom, či právo Spojených štátov skutočne zaručuje primeranú úroveň ochrany vyžadovanú článkom 45 nariadenia GDPR v spojení so základnými právami zaručenými v článkoch 7, 8 a 47 Charty. Uvedený súd sa konkrétne domnieva, že právo tejto tretej krajiny nestanovuje nevyhnutné obmedzenia a záruky vo vzťahu

k zásahom povoleným jeho vnútroštátnou právnou úpravou a ani nezabezpečuje účinnú súdnu ochranu pred takými zásahmi. V tejto súvislosti dodáva, že zriadenie ombudsmana pre štít na ochranu údajov nemôže podľa tohto súdu napraviť dané nedostatky, keďže tohto ombudsmana nemožno považovať za súd v zmysle článku 47 Charty.

169 Pokiaľ ide v prvom rade o články 7 a 8 Charty, ktoré prispievajú k dosiahnutiu požadovanej úrovne ochrany v rámci Únie a ktorých dodržanie musí Komisia konštatovať pred prijatím rozhodnutia o primeranosti podľa článku 45 ods. 1 nariadenia GDPR, treba pripomenúť, že článok 7 Charty zaručuje každému právo na rešpektovanie jeho súkromného a rodinného života, obydlia a komunikácie. Článok 8 ods. 1 Charty navyše každému výslovne priznáva právo na ochranu osobných údajov, ktoré sa ho týkajú.

170 Prístup k osobným údajom fyzickej osoby s cieľom ich uchovávania alebo ich použitia má teda vplyv na základné právo tejto osoby na rešpektovanie súkromného života zaručené v článku 7 Charty, keďže toto právo sa vzťahuje na všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Na uvedené spracovanie údajov sa vzťahuje článok 8 Charty z dôvodu, že predstavuje spracovanie osobných údajov v zmysle tohto článku, a teda nevyhnutne musí spĺňať požiadavky ochrany údajov, ktoré stanovuje uvedený článok [pozri v tomto zmysle rozsudky z 9. novembra 2010, Volker und Markus Schecke a Eifert, C-92/09 a C-93/09, EU:C:2010:662, body 49 a 52; z 8. apríla 2014, Digital Rights Ireland a i., C-293/12 a C-594/12, EU:C:2014:238, bod 29, ako aj stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 122 a 123].

171 Súdny dvor už rozhodol, že poskytnutie osobných údajov tretej osobe, akou je orgán verejnej moci, predstavuje zásah do základných práv zakotvených v článkoch 7 a 8 Charty bez ohľadu na neskoršie použitie poskytnutých informácií. To isté platí s ohľadom na uchovávanie osobných údajov, ako aj prístup k uvedeným údajom na účely ich použitia orgánmi verejnej moci, nezávisle od toho, či dotknuté informácie týkajúce sa súkromného života majú alebo nemajú citlivú povahu alebo či pre dotknuté osoby z dôvodu tohto zásahu vyplynuli alebo nevyplynuli prípadné nepriaznivé následky [pozri v tomto zmysle rozsudky z 20. mája 2003, Österreichischer Rundfunk a i., C-465/00, C-138/01 a C-139/01, EU:C:2003:294, body 74 a 75; z 8. apríla 2014, Digital Rights Ireland a i., C-293/12 a C-594/12, EU:C:2014:238, body 33 až 36, ako aj stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 124 a 126].

172 Práva zakotvené v článkoch 7 a 8 Charty však nie sú absolútnymi výsadami, ale musia sa vnímať vo vzťahu k ich úlohe v spoločnosti [pozri v tomto zmysle rozsudky z 9. novembra 2010, Volker und Markus Schecke a Eifert, C-92/09 a C-93/09, EU:C:2010:662, bod 48 a citovanú judikatúru; zo 17. októbra 2013, Schwarz, C-291/12, EU:C:2013:670, bod 33 a citovanú judikatúru, ako aj stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 136].

173 V tejto súvislosti treba tiež uviesť, že podľa článku 8 ods. 2 Charty musia byť osobné údaje spracované najmä „na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom“.

174 Okrem toho podľa článku 52 ods. 1 prvej vety Charty, akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto Charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Podľa článku 52 ods. 1 druhej vety Charty možno pri dodržaní zásady proporcionality tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.

175 V tejto súvislosti treba dodať, že požiadavka, podľa ktorej musí byť každé obmedzenie výkonu základných práv stanovené zákonom, predpokladá, že samotný právny základ, ktorý umožňuje zásah do týchto práv, musí vymedzovať rozsah obmedzenia výkonu dotknutého práva [stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 139 a citovaná judikatúra].

176 Napokon na splnenie požiadavky proporcionality, podľa ktorej výnimky z ochrany osobných údajov a jej obmedzenia musia pôsobiť v rámci toho, čo je striktne nevyhnutné, musí dotknutá právna úprava obsahujúca zásah stanoviť jasné a presné pravidlá, ktoré budú upravovať rozsah a uplatnenie predmetného opatrenia a ukladať minimálne požiadavky tak, aby osoby, ktorých údaje boli prenesené, mali dostatočné záruky umožňujúce im účinne chrániť ich osobné údaje pred rizikami zneužitia. Táto právna úprava musí najmä vymedziť okolnosti a podmienky, za akých možno prijať opatrenie upravujúce spracovanie takýchto údajov, čím zaručí, aby zásah nešiel nad rámec toho, čo je striktne nevyhnutné. Nevyhnutnosť disponovať takými zárukami je o to dôležitejšia v prípade, keď sú osobné údaje spracúvané automaticky [pozri v tomto zmysle stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou), z 26. júla 2017, EU:C:2017:592, body 140 a 141, ako aj citovanú judikatúru].

177 V tejto súvislosti článok 45 ods. 2 písm. a) nariadenia GDPR spresňuje, že Komisia v rámci svojho posúdenia primeranosti úrovne ochrany zabezpečovanej treťou krajinou zohľadní najmä „účinné a vymáhateľné práva… pre dotknuté osoby“, ktorých osobné údaje sa prenášajú.

178 V prejednávanej veci bolo zistenie Komisie v rozhodnutí ŠnOOÚ, podľa ktorého Spojené štáty zabezpečujú úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie na základe nariadenia GDPR v spojení s článkami 7 a 8 Charty, spochybnené najmä z dôvodu, že zásahy vyplývajúce z programov sledovania založených na článku 702 FISA a E.O. 12333 nepodliehajú požiadavkám, ktoré pri dodržaní zásady proporcionality zabezpečujú úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej článkom 52 ods. 1 druhou vetou Charty. Treba teda preskúmať, či sa tieto programy sledovania vykonávajú v súlade s takými požiadavkami bez toho, aby bolo potrebné najprv overiť, či táto tretia krajina spĺňa podmienky, ktoré sú v podstate rovnocenné podmienkam stanoveným v článku 52 ods. 1 prvej vete Charty.

179 V tejto súvislosti, pokiaľ ide o programy sledovania založené na článku 702 FISA, Komisia v odôvodnení 109 rozhodnutia ŠnOOÚ konštatovala, že podľa uvedeného článku „FISC… nepovoľuje jednotlivé opatrenia sledovania; povoľuje skôr programy sledovania (ako PRISM, UPSTREAM) na základe každoročných certifikácií pripravených generálnym prokurátorom [United States General Attorney] a riaditeľom národnej spravodajskej služby [Director of National Intelligence (DNI)]“. Ako vyplýva z tohto odôvodnenia, cieľom kontroly vykonávanej FISC je teda overiť, či tieto programy sledovania zodpovedajú cieľu získať informácie v oblasti zahraničných spravodajských informácií, ale nezaoberá sa tým, „či boli osoby správne zacielené s cieľom získať zahraničné spravodajské informácie“.

180 Zdá sa teda, že z článku 702 FISA nijako nevyplýva existencia obmedzení oprávnenia, ktoré obsahuje a ktorým sa vykonávajú programy sledovania na účely zahraničných spravodajských informácií, ani existencia záruk pre osoby, ktoré nie sú americkými občanmi a ktorých sa môžu týkať tieto programy. Za týchto podmienok a ako v podstate uviedol generálny advokát v bodoch 291, 292 a 297 svojich návrhov, tento článok nemôže zabezpečiť úroveň ochrany, ktorá je v podstate rovnocenná s úrovňou zaručenou Chartou, ako ju vykladá judikatúra pripomenutá v bodoch 175 a 176 tohto rozsudku, podľa ktorej samotný právny základ, ktorý umožňuje zásah do základných práv, musí na účely splnenia zásady proporcionality sám definovať rozsah obmedzenia výkonu dotknutého práva a stanoviť jasné a presné pravidlá, ktoré budú upravovať rozsah a uplatnenie predmetného opatrenia a ukladať minimálne požiadavky.

181 Podľa zistení uvedených v rozhodnutí ŠnOOÚ sa programy sledovania založené na článku 702 FISA musia vykonávať v súlade s požiadavkami vyplývajúcimi z PPD-28. Hoci Komisia v odôvodneniach 69 a 77 rozhodnutia ŠnOOÚ zdôraznila, že také požiadavky majú pre spravodajské služby Spojených štátov záväzný charakter, americká vláda v odpovedi na otázku Súdneho dvora pripustila, že PPD-28 nepriznáva dotknutým osobám práva uplatniteľné pred súdmi voči americkým orgánom. Preto nemôže zabezpečiť úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany vyplývajúcej z Charty, na

rozdiel od toho, čo vyžaduje článok 45 ods. 2 písm. a) nariadenia GDPR, podľa ktorého konštatovanie tejto úrovne závisí najmä od existencie skutočných a vymožiteľných práv prináležiacich osobám, ktorých údaje boli prenesené do dotknutej tretej krajiny.

182 Pokiaľ ide o programy sledovania založené na E.O. 12333, zo spisu, ktorý má Súdny dvor k dispozícii, vyplýva, že ani toto nariadenie nepriznáva práva uplatniteľné pred súdmi voči americkým orgánom.

183 Je potrebné dodať, že PPD-28, ktorá sa musí dodržiavať pri vykonávaní programov uvedených v predchádzajúcich dvoch bodoch, umožňuje „‚hromadné zhromažďovanie'… pomerne veľkého objemu informácií alebo údajov prostredníctvom signálového spravodajstva za okolností, keď spravodajské služby nemôžu použiť identifikátor spojený s konkrétnym cieľom…, aby mohli presne zamerať zhromažďovanie informácií", ako sa uvádza v liste od Úradu riaditeľa národnej spravodajskej služby Ministerstvu obchodu USA, ako aj správnemu orgánu zahraničného obchodu z 21. júna 2016, ktorý sa nachádza v prílohe VI rozhodnutia ŠnOOÚ. Táto možnosť, ktorá v rámci programov sledovania založených na E.O. 12333 umožňuje prístup k údajom na ceste do Spojených štátov bez toho, aby podliehal tento prístup akémukoľvek preskúmaniu zo strany súdov, však v žiadnom prípade dostatočne jasne a presne nevymedzuje rozsah hromadného zhromažďovania osobných údajov.

184 Zdá sa teda, že ani článok 702 FISA, ani E.O. 12333 v spojení s PPD-28 nezodpovedajú minimálnym požiadavkám, ktoré sú v práve Únie spojené so zásadou proporcionality, takže nemožno dospieť k záveru, že programy sledovania založené na týchto ustanoveniach sa obmedzujú na to, čo je striktne nevyhnutné.

185 Za týchto podmienok obmedzenia ochrany osobných údajov, ktoré vyplývajú z vnútroštátnej právnej úpravy Spojených štátov týkajúcej sa prístupu a používania takýchto údajov prenášaných z Únie do Spojených štátov americkými orgánmi verejnej moci a ktoré Komisia posúdila v rozhodnutí ŠnOOÚ, nie sú vymedzené takým spôsobom, aby zodpovedali požiadavkám, ktoré sú v podstate rovnocenné požiadavkám vyžadované v práve Únie v článku 52 ods. 1 druhej vete Charty.

186 Pokiaľ ide v druhom rade o článok 47 Charty, ktorý tiež prispieva k úrovni ochrany požadovanej v rámci Únie a ktorého dodržanie musí Komisia konštatovať skôr, než prijme rozhodnutie o primeranosti podľa článku 45 ods. 1 nariadenia GDPR, treba pripomenúť, že prvý odsek tohto článku 47 vyžaduje, aby každý, koho práva a slobody zaručené právom Únie boli porušené, mal za podmienok ustanovených v tomto článku právo na účinný prostriedok nápravy pred súdom. V zmysle znenia druhého odseku daného článku má každý právo na to, aby jeho záležitosť bola prejednaná nezávislým a nestranným súdom.

187 Podľa ustálenej judikatúry samotná existencia účinného súdneho preskúmavania na účely dodržania ustanovení práva Únie je súčasťou existencie právneho štátu. Právna úprava, ktorá neupravuje nijakú možnosť osoby podliehajúcej súdnej právomoci uplatniť právne prostriedky nápravy, aby mala prístup k osobným údajom, ktoré sa jej týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov, tak nerešpektuje podstatu obsahu základného práva na účinnú súdnu ochranu, ako je upravené článkom 47 Charty (rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 95, a citovaná judikatúra).

188 V tejto súvislosti článok 45 ods. 2 písm. a) nariadenia GDPR vyžaduje, aby Komisia v rámci svojho posúdenia primeranosti úrovne ochrany zabezpečovanej treťou krajinou zohľadnila najmä „účinné a vymáhateľné práva dotknutej osoby a účinné správne a súdne prostriedky nápravy pre dotknuté osoby, ktorých osobné údaje sa prenášajú". Odôvodnenie 104 nariadenia GDPR v tejto súvislosti zdôrazňuje, že tretia krajina „by predovšetkým mala zabezpečiť účinný a nezávislý dozor nad ochranou údajov, ako aj mechanizmy spolupráce s orgánmi členských štátov na ochranu údajov" a spresňuje, že „dotknutým osobám by sa mali poskytnúť účinné a vymožiteľné práva a účinné správne a súdne prostriedky nápravy".

189 Existencia takýchto účinných prostriedkov nápravy v dotknutej tretej krajine má osobitný význam v súvislosti s prenosom osobných údajov do uvedenej tretej krajiny, keďže ako vyplýva z odôvodnenia 116 nariadenia GDPR, dotknuté osoby sa môžu dostať do situácie, že správne a súdne orgány členských štátov nebudú mať dostatok právomocí a prostriedkov na to, aby mohli užitočne konať vo veciach sťažností uvedených osôb založených na údajnom protiprávnom spracúvaní ich údajov v tejto tretej krajine, ktoré sú takto prenášané, čo ich môže nútiť k tomu, aby sa obrátili na vnútroštátne orgány a súdy danej tretej krajiny.

190 V prejednávanej veci bolo zistenie Komisie v rozhodnutí ŠnOOÚ, podľa ktorého Spojené štáty zabezpečujú úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej článkom 47 Charty, spochybnené najmä z dôvodu, že zriadenie ombudsmana pre štít na ochranu osobných údajov nemôže napraviť nedostatky konštatované samotnou Komisiou, pokiaľ ide o súdnu ochranu osôb, ktorých osobné údaje sa do tejto tretej krajiny prenášajú.

191 V tejto súvislosti Komisia v bode 115 rozhodnutia ŠnOOÚ uviedla, že „hoci teda fyzické osoby vrátane dotknutých osôb z [Únie] majú niekoľko možností nápravy, keď sa stali predmetom nezákonného (elektronického) sledovania na účely národnej bezpečnosti, je jasné aj to, že tieto možnosti sa nevzťahujú aspoň na niektoré právne základy, ktoré spravodajské orgány USA môžu využiť (napr. vykonávacie nariadenie [E.O.] č. 12333)“. Pokiaľ teda ide o E.O. 12333, v uvedenom odôvodnení 115 zdôraznila neexistenciu akéhokoľvek práva na možnosť nápravy. Podľa judikatúry pripomenutej v bode 187 tohto rozsudku však takáto medzera v súdnej ochrane, pokiaľ ide o zásahy spojené s programami sledovania založenými na tomto vykonávacom nariadení, bráni záveru, ktorý urobila Komisia v rozhodnutí ŠnOOÚ, že právo Spojených štátov zaručuje úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej článkom 47 Charty.

192 Okrem toho, čo sa týka programov sledovania založených na článku 702 FISA, ako aj programov založených na E.O. 12333, v bodoch 181 a 182 tohto rozsudku bolo uvedené, že ani PPD-28, ani E.O. 12333 nepriznávajú dotknutým osobám práva uplatniteľné pred súdmi voči americkým orgánom, takže tieto osoby nemajú právo na účinný prostriedok nápravy.

193 Komisia napriek tomu v odôvodneniach 115 a 116 rozhodnutia ŠnOOÚ konštatovala, že z dôvodu existencie mechanizmu ombudsmana zavedeného americkými orgánmi, ako je opísaný v liste zaslanom 7. júla 2016 ministrom zahraničných vecí Spojených štátov Európskej komisárke pre spravodlivosť, spotrebiteľov a rodovú rovnosť, ktorý je uvedený v prílohe III tohto rozhodnutia, a na základe povahy úlohy zverenej ombudsmanovi, v danom prípade „hlavnému koordinátorovi medzinárodnej diplomacie v oblasti informačných technológií“ Spojených štátov, táto krajina môže byť považovaná za zabezpečujúcu úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej článkom 47 Charty.

194 Preskúmanie otázky, či mechanizmus ombudsmana uvedený v rozhodnutí ŠnOOÚ môže skutočne napraviť obmedzenia práva na súdnu ochranu konštatované Komisiou, musí v súlade s požiadavkami vyplývajúcimi z článku 47 Charty a z judikatúry pripomenutej v bode 187 tohto rozsudku vychádzať zo zásady, že osoby podliehajúce súdnej právomoci musia mať možnosť uplatniť právne prostriedky nápravy pred nezávislým a nestranným súdom, aby mali prístup k osobným údajom, ktoré sa ich týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov.

195 V liste spomenutom v bode 193 tohto rozsudku bol ombudsman pre štít na ochranu osobných údajov, hoci je opísaný ako „nezávislý od spravodajských služieb“, predstavený tak, že „podlieha priamo ministrovi zahraničných vecí, ktorý zabezpečí, aby ombudsman vykonával svoju funkciu objektívne a bez pôsobenia neprimeraných vplyvov, ktoré by mohli viesť k ovplyvňovaniu poskytovanej odpovede“. Navyše okrem skutočnosti, ako konštatovala Komisia v odôvodnení 116 tohto rozhodnutia, že ombudsman je menovaný ministrom zahraničných vecí a je neoddeliteľnou súčasťou Ministerstva zahraničných vecí Spojených štátov, neexistuje v uvedenom rozhodnutí – ako uviedol generálny advokát v bode 337 svojich návrhov – žiadna zmienka o tom, že by sa s odvolaním ombudsmana

alebo zrušením jeho vymenovania spájali osobitné záruky, čo môže spochybňovať nezávislosť ombudsmana vo vzťahu k výkonnej moci (pozri v tomto zmysle rozsudok z 21. januára 2020, Banco de Santander, C-274/14, EU:C:2020:17, body 60 a 63, ako aj citovanú judikatúru).

196 Rovnako, ako zdôraznil generálny advokát v bode 338 svojich návrhov, hoci odôvodnenie 120 rozhodnutia ŠnOOÚ poukazuje na záväzok americkej vlády, že príslušná zložka spravodajských služieb bude povinná napraviť všetky porušenia platných predpisov, ktoré ombudsman pre štít na ochranu osobných údajov zistí, uvedené rozhodnutie neuvádza nijaké ustanovenie, podľa ktorého by tento ombudsman bol oprávnený voči týmto službám prijímať záväzné rozhodnutia, ani nestanovuje zákonné záruky, ktoré by boli s týmto záväzkom spojené a ktorých by sa dotknuté osoby mohli dovolávať.

197 Mechanizmus ombudsmana uvedený v rozhodnutí ŠnOOÚ teda neposkytuje opravný prostriedok pred orgánom, ktorý by ponúkal osobám, ktorých údaje sa prenášajú do Spojených štátov, záruky, ktoré sú v podstate rovnocenné zárukám vyžadovaným podľa článku 47 Charty.

198 Komisia teda tým, že v článku 1 ods. 1 rozhodnutia ŠnOOÚ konštatovala, že Spojené štáty zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám usadeným v tejto tretej krajine v rámci štítu na ochranu osobných údajov medzi Európskou úniou a USA, porušila požiadavky vyplývajúce z článku 45 ods. 1 nariadenia GDPR v spojení s článkami 7, 8 a 47 Charty.

199 Z toho vyplýva, že článok 1 rozhodnutia ŠnOOÚ je nezlučiteľný s článkom 45 ods. 1 nariadenia GDPR v spojení s článkami 7, 8 a 47 Charty a je z tohto dôvodu neplatný.

200 Keďže článok 1 rozhodnutia ŠnOOÚ je neoddeliteľný od článkov 2 až 6, ako aj od jeho príloh, jeho neplatnosť má vplyv na platnosť tohto rozhodnutia ako celku.

201 Vzhľadom na vyššie uvedené úvahy treba dospieť k záveru, že rozhodnutie ŠnOOÚ je neplatné.

202 Pokiaľ ide o otázku, či treba zachovať účinky tohto rozhodnutia, aby sa zamedzilo vzniku právneho vákua (pozri v tomto zmysle rozsudok z 28. apríla 2016, Borealis Polyolefine a i., C-191/14, C-192/14, C-295/14, C-389/14 a C-391/14 až C-393/14, EU:C:2016:311, bod 106), treba poznamenať, že v každom prípade vzhľadom na článok 49 nariadenia GDPR zrušenie rozhodnutia o primeranosti, akým je rozhodnutie ŠnOOÚ, nemôže viesť k vzniku takéhoto právneho vákua. Tento článok totiž presne stanovuje podmienky, za akých sa prenosy osobných údajov do tretích krajín môžu uskutočniť bez rozhodnutia o primeranosti podľa článku 45 ods. 3 uvedeného nariadenia alebo primeraných záruk podľa článku 46 toho istého nariadenia.

O trovách

203 Vzhľadom na to, že konanie pred Súdnym dvorom má vo vzťahu k účastníkom konania vo veci samej incidenčný charakter a bolo začaté v súvislosti s prekážkou postupu v konaní pred vnútroštátnym súdom, o trovách konania rozhodne tento vnútroštátny súd. Iné trovy konania, ktoré vznikli v súvislosti s predložením pripomienok Súdnemu dvoru a nie sú trovami uvedených účastníkov konania, nemôžu byť nahradené.

Z týchto dôvodov Súdny dvor (veľká komora) rozhodol takto:

1. **Článok 2 ods. 1 a 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa ruší smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), sa má vykladať v tom zmysle, že do pôsobnosti tohto nariadenia patrí prenos osobných údajov vykonaný na obchodné účely hospodárskym subjektom usadeným v jednom členskom štáte**

inému hospodárskemu subjektu usadenému v tretej krajine bez ohľadu na to, či v priebehu tohto prenosu alebo po ňom môžu byť tieto údaje spracúvané orgánmi dotknutej tretej krajiny na účely verejnej bezpečnosti, obrany a bezpečnosti štátu.

2. **Článok 46 ods. 1 a článok 46 ods. 2 písm. c) nariadenia 2016/679 sa majú vykladať v tom zmysle, že primerané záruky, vymožiteľné práva a účinné právne prostriedky nápravy vyžadované týmito ustanoveniami musia zabezpečiť, aby práva osôb, ktorých osobné údaje sa prenášajú do tretej krajiny na základe štandardných doložiek o ochrane údajov, požívali úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Európskej únie týmto nariadením v spojení s Chartou základných práv Európskej únie. Na tento účel posúdenie úrovne ochrany zaručenej v kontexte takéhoto prenosu musí najmä zohľadniť tak zmluvné ustanovenia dohodnuté medzi prevádzkovateľom alebo jeho sprostredkovateľom usadeným v Únii a príjemcom prenosu usadeným v dotknutej tretej krajine, ako aj, pokiaľ ide o prípadný prístup orgánov verejnej moci tejto tretej krajiny k takto prenášaným osobným údajom, relevantné prvky právneho systému tejto krajiny, najmä tie, ktoré sú uvedené v článku 45 ods. 2 uvedeného nariadenia.**

3. **Článok 58 ods. 2 písm. f) a j) nariadenia 2016/679 sa má vykladať v tom zmysle, že pokiaľ neexistuje rozhodnutie o primeranosti, ktoré Európska komisia platne prijala, príslušný dozorný orgán je povinný pozastaviť alebo zakázať prenos osobných údajov do tretej krajiny založený na štandardných doložkách o ochrane údajov prijatých Komisiou, ak sa tento dozorný orgán vzhľadom na všetky osobitné okolnosti tohto prenosu domnieva, že tieto doložky nie sú alebo nemôžu byť v tejto tretej krajine dodržané a že ochrana prenášaných údajov, ktorú vyžaduje právo Únie, najmä články 45 a 46 tohto nariadenia, ako aj Charta základných práv Európskej únie, nemôže byť zabezpečená inými prostriedkami, pokiaľ prevádzkovateľ alebo jeho sprostredkovateľ so sídlom v Únii sám tento prenos nepozastaví alebo neukončí.**

4. **Preskúmanie rozhodnutia Komisie 2010/87/EÚ z 5. februára 2010 o štandardných zmluvných doložkách pre prenos osobných údajov spracovateľom usadeným v tretích krajinách podľa smernice Európskeho parlamentu a Rady 95/46/ES, zmeneného vykonávacím rozhodnutím Komisie (EÚ) 2016/2297 zo 16. decembra 2016, vzhľadom na články 7, 8 a 47 Charty základných práv Európskej únie neodhalilo nijakú skutočnosť, ktorá by mohla ovplyvniť platnosť tohto rozhodnutia.**

5. **Vykonávacie rozhodnutie Komisie (EÚ) 2016/1250 z 12. júla 2016 podľa smernice Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA je neplatné.**

Podpisy