



PRIJATÉ TEXTY

P8_TA(2018)0529

Primeranosť ochrany osobných údajov zo strany Japonska

Uznesenie Európskeho parlamentu z 13. decembra 2018 o primeranosti ochrany osobných údajov zo strany Japonska (2018/2979(RSP))

Európsky parlament,

- so zreteľom na Zmluvu o Európskej únii, Zmluvu o fungovaní Európskej únie a na články 6, 7, 8, 11, 16, 47 a 52 Charty základných práv Európskej únie,
- so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)¹, a na ďalšie relevantné európske *acquis* o ochrane údajov,
- so zreteľom na rozsudok Súdneho dvora Európskej únie zo 6. októbra 2015 vo veci C-362/14 (Maximillian Schrems/Data Protection Commissioner)²,
- so zreteľom na rozsudok Súdneho dvora Európskej únie z 21. decembra 2016 v spojených veciach C-203/15 (Tele 2 Sverige AB proti Post- och telestyrelsen) a C-698/15 (Secretary of State for the Home Department proti Tomovi Watsonovi a iným)³,
- so zreteľom na svoje uznesenie z 12. decembra 2017 s názvom Smerom k stratégii digitálneho obchodu⁴,
- so zreteľom na dokument pracovnej skupiny zriadenej podľa článku 29 s názvom Referenčné kritérium primeranosti zo 6. februára 2018⁵, ktorý poskytuje Komisii a Európskemu výboru pre ochranu údajov usmernenia podľa všeobecného nariadenia o ochrane údajov na posúdenie úrovne ochrany údajov v tretích krajinách a medzinárodných organizáciách,
- so zreteľom na stanovisko Európskeho výboru pre ochranu údajov z 5. decembra 2018 k

¹ Ú. v. EÚ L 119, 4.5.2016, s. 1.

² ECLI:EU:C:2015:650.

³ ECLI:EU:C:2016:970.

⁴ Ú. v. EÚ C 369, 11.10.2018, s. 22.

⁵ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108; schválený Európskym výborom pre ochranu údajov na jeho prvom plenárnom zasadnutí.

návrhu rozhodnutia o primeranosti medzi EÚ a Japonskom,

- so zreteľom na návrh vykonávacieho rozhodnutia Komisie podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o primeranej ochrane osobných údajov zo strany Japonska (COM(2018)XXXX),
 - so zreteľom na zistenia návštevy ad hoc delegácie Výboru pre občianske slobody, spravodlivosť a vnútorné veci v Japonsku, ktorá sa uskutočnila v októbri 2017 v rámci rokovaní o primeranosti a ktorej cieľom bolo stretnúť sa s príslušnými japonskými orgánmi a zainteresovanými stranami v súvislosti so základnými prvkami, ktoré má Komisia zvážiť pri prijímaní rozhodnutia o primeranosti,
 - so zreteľom na článok 123 ods. 2 rokovacieho poriadku,
- A. keďže všeobecné nariadenie o ochrane údajov sa uplatňuje od 25. mája 2018; keďže článok 45 ods. 2 všeobecného nariadenia o ochrane údajov stanovuje prvky, ktoré má Komisia zohľadniť pri posudzovaní primeranosti úrovne ochrany v tretej krajine alebo medzinárodnej organizácii;
- B. keďže Komisia musí brať na zreteľ najmä zásady právneho štátu, dodržiavanie ľudských práv a základných slobôd, relevantné všeobecné aj odvetvové právne predpisy vrátane právnych predpisov týkajúcich sa verejnej bezpečnosti, obrany, národnej bezpečnosti, trestného práva a prístupu verejných orgánov k osobným údajom, existenciu a účinné fungovanie jedného alebo viacerých nezávislých orgánov dohľadu a medzinárodné záväzky, ktoré tretia krajina alebo medzinárodná organizácia prijala;
- C. keďže Súdny dvor EÚ vo svojom rozsudku zo 6. októbra 2015 vo veci C-362/14 (Maximilian Schrems/Data Protection Commissioner) objasnil, že primeraná úroveň ochrany v tretej krajine sa musí chápať ako „v podstate rovnocenná“ úrovni ochrany zaručenej v rámci Európskej únie na základe smernice 95/46/ES v spojení s chartou;
- D. keďže Japonsko je jedným z kľúčových obchodných partnerov EÚ, s ktorým nedávno uzatvorila dohodu o hospodárskom partnerstve (DHP), v ktorej sú zakotvené spoločné hodnoty a zásady a zároveň sa v nej upravujú citlivé záležitosti oboch partnerov; keďže spoločné uznávanie základných práv vrátane ochrany súkromia a údajov predstavuje dôležitý základ pre rozhodnutie o primeranosti, ktoré poskytne právny základ pre prenos osobných údajov z EÚ do Japonska;
- E. keďže ad hoc delegácia Výboru pre občianske slobody, spravodlivosť a vnútorné veci do Japonska bola informovaná o záujme japonských orgánov a zainteresovaných strán, nielen pokiaľ ide o uplatňovanie samotných nových pravidiel všeobecného nariadenia o ochrane údajov, ale aj o vytvorenie pevného mechanizmu prenosu osobných údajov na vysokej úrovni medzi EÚ a Japonskom, ktorý by splňal podmienky stanovené v právnom rámci EÚ z hľadiska úrovne ochrany, ktorá sa v podstate považuje za rovnocennú úrovni ochrany, ktorú poskytujú právne predpisy EÚ v oblasti ochrany údajov;
- F. keďže prenos osobných údajov medzi EÚ a Japonskom na obchodné účely je dôležitým prvkom týchto dvojstranných vzťahov vzhľadom na neprestajne rastúcu digitalizáciu globálnej ekonomiky; keďže tento prenos by mal byť vykonávaný pri plnom rešpektovaní práva na ochranu osobných údajov a práva na súkromie; keďže jedným zo

základných cieľov EÚ je ochrana základných práv zakotvených v Charte základných práv Európskej únie;

- G. keďže EÚ a Japonsko začali v januári 2017 diskusie, ktorých cieľom bolo uľahčiť prenos osobných údajov na obchodné účely prostredníctvom vôbec prvého „získovania o vzájomnej primeranosti“; keďže Európsky parlament vo svojom uznesení z 12. decembra 2017 s názvom Smerom k stratégii digitálneho obchodu výslovne uznáva, že „rozhodnutia o primeranosti [...] sú základným nástrojom na ochranu prenosu osobných údajov z EÚ do tretej krajiny“;
- H. keďže rozhodnutie o primeranosti týkajúce sa prenosu osobných údajov do Japonska by bolo prvým takýmto rozhodnutím prijatým podľa nových a prísnejších pravidiel všeobecného nariadenia o ochrane údajov;
- I. keďže Japonsko nedávno zmodernizovalo a posilnilo svoje právne predpisy o ochrane údajov s cieľom zosúladiť ich s medzinárodnými normami, najmä so zárukami a individuálnymi právami stanovenými v novom európskom legislatívnom rámci pre ochranu údajov; keďže japonský právny rámec na ochranu údajov pozostáva z rôznych pilierov, pričom hlavným právnym predpisom je zákon o ochrane osobných informácií (Act on Protection of Personal Information – APPI);
- J. keďže vláda Japonska 12. júna 2018 prijala nariadenie vlády, na základe ktorého sa na komisiu pre ochranu osobných informácií (Personal Information Protection Commission – PPC) ako orgán zodpovedný za správu a vykonávanie zákona APPI deleguje „právu prijímať potrebné opatrenia na preklenutie rozdielov v systémoch a operáciách medzi Japonskom a príslušnou cudzou krajinou na základe článku 6 daného zákona s cieľom zabezpečiť primerané zaobchádzanie s osobnými informáciami získanými z tejto krajiny“; keďže v tomto rozhodnutí sa uvádza, že v tom je zahrnutá právomoc stanoviť posilnenú ochranu tým, že komisia PPC prijme prísnejšie pravidlá, ktorými sa doplnia pravidlá stanovené v APPI a v nariadení vlády a prekročí sa ich rámec; keďže podľa tohto rozhodnutia by tieto prísnejšie pravidlá boli záväzné a vymáhateľné voči japonským prevádzkovateľom podnikov;
- K. keďže k návrhu vykonávacieho rozhodnutia Komisie o primeranej ochrane osobných údajov zo strany Japonska sú v prílohe I pripojené doplňujúce pravidlá prijaté komisiou PPC 15. júna 2018, ktoré sú založené na článku 6 APPI, čo výslovne umožňuje PPC prijať prísnejšie pravidlá, a to aj na účely uľahčenia medzinárodných prenosov údajov; keďže doplňujúce pravidlá ešte nie sú verejne dostupné;
- L. keďže účelom týchto doplňujúcich pravidiel by bolo riešiť príslušné rozdiely medzi japonskými právnymi predpismi a právnymi predpismi EÚ o ochrane údajov s cieľom zabezpečiť primerané zaobchádzanie s osobnými informáciami získanými z EÚ na základe rozhodnutia o primeranosti, najmä pokiaľ ide o osobné informácie vyžadujúce si osobitné zaobchádzanie (citlivé údaje), uchovávané osobné údaje, špecifikovanie účelu využitia, obmedzenie z dôvodu účelu využitia, obmedzenie poskytovania tretej strane v cudzej krajine a anonymne spracovávané informácie;
- M. keďže doplňujúce pravidlá by boli právne záväzné pre každý podnikateľský subjekt spracúvajúci osobné informácie, ktorý prijíma osobné údaje prenášané z EÚ na základe rozhodnutia o primeranosti, a je preto povinný tieto pravidlá a akékoľvek súvisiace práva a povinnosti dodržiavať, a vykonateľné zo strany komisie PPC aj japonských

súdob;

- N. keďže s cieľom zabezpečiť v podstate rovnocennú úroveň ochrany osobných údajov prenášaných z EÚ do Japonska vytvárajú doplňujúce pravidlá dodatočnú ochranu, ktorá sa má uplatňovať na základe prísnejších podmienok alebo obmedzení spracúvania osobných údajov prenášaných z EÚ, napríklad v prípade osobných informácií vyžadujúcich osobitné zaobchádzanie, následných prenosov, anonymných údajov a obmedzenia účelu;
- O. keďže japonský právny rámec na ochranu údajov rozlišuje medzi „osobnými informáciami“ a „osobnými údajmi“ a v niektorých prípadoch odkazuje na špecifickú kategóriu osobných údajov, konkrétne na „uchovávané osobné údaje“;
- P. keďže podľa článku 2 ods. 1 APPI pojem „osobné informácie“ zahŕňa všetky informácie týkajúce sa živej osoby, ktoré umožňujú identifikáciu tejto osoby; keďže vo vymedzení sa rozlišujú dve kategórie osobných informácií, a to i) individuálne identifikačné kódy a ii) iné osobné informácie, na základe ktorých možno konkrétnu osobu identifikovať; keďže táto druhá kategória zahŕňa informácie, ktoré samotné neumožňujú identifikáciu konkrétnej osoby, avšak môžu ju umožniť v prípade, že sa jednoducho pospájajú s inými informáciami;
- Q. keďže podľa článku 2 ods. 4 APPI „osobné údaje“ znamenajú osobné informácie, ktoré tvoria databázu osobných údajov atď.; keďže v článku 2 ods. 1 APPI sa stanovuje, že informácie v týchto databázach sa systematizujú, čo je podobné koncepcii informačného systému podľa článku 2 ods. 1 všeobecného nariadenia o ochrane údajov; keďže podľa čl. 4 ods. 1 všeobecného nariadenia o ochrane údajov „osobné údaje“ znamenajú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby; keďže identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje alebo online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby; keďže na určenie toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby;
- R. keďže podľa článku 2 ods. 7 APPI „uchovávané osobné údaje“ znamenajú osobné údaje, ktoré má podnikateľský subjekt zaobchádzajúci s osobnými informáciami právomoc zverejniť, opraviť, doplniť alebo vymazať ich obsah, ukončiť ich využívanie, vymazať alebo ukončiť ich poskytovanie tretej strane, pričom nejde o údaje, ktoré podľa vládneho nariadenia môžu poškodiť verejný alebo iný záujem, ak sa ich prítomnosť alebo absencia zverejní, ani o údaje, ktoré sa majú podľa nariadenia vlády vymazať v lehote, ktorá nie je dlhšia ako jeden rok; keďže doplňujúce pravidlá zosúladzujú pojem „uchovávané osobné údaje“ s pojmom „osobné údaje“, aby sa zabezpečilo, že určité obmedzenia individuálnych práv, ktoré sú s týmito údajmi spojené, sa nebudú vzťahovať na údaje prenášané z EÚ;
- S. keďže japonský právny predpis o ochrane údajov, ktorý je predmetom návrhu vykonávacieho rozhodnutia, z rozsahu svojej pôsobnosti vylučuje viaceré odvetvia, keď spracúvajú osobné údaje na osobitné účely; keďže návrh vykonávacieho rozhodnutia by

sa nevzťahoval na prenos osobných údajov z EÚ príjemcovi, ktorý patrí do ktorejkoľvek z uvedených výnimiek stanovených v japonskom právnom predpise o ochrane údajov;

- T. keďže pokiaľ ide o následné prenosy osobných údajov EÚ z Japonska do tretej krajiny, návrh vykonávacieho rozhodnutia vylučuje možnosť, aby sa na takéto následné prenosy použili nástroje prenosu, ktoré nevytvárajú záväzný vzťah medzi japonským vývozcom údajov a dovozcom údajov z tretej krajiny a nezaručujú požadovanú úroveň ochrany; keďže by to tak bolo napríklad v prípade systému Ázijsko-tichomorskej hospodárskej spolupráce v oblasti cezhraničných pravidiel ochrany súkromia (APEC CBPR), v ktorom je Japonsko účastníckou ekonomikou, pretože v tomto systéme ochrana nevyplýva z dohody, ktorá je záväzná pre vývozcu a dovozcu v kontexte ich dvojstranného vzťahu, a je jednoznačne na nižšej úrovni, ako je úroveň zaručená kombináciou zákona APPI a doplňujúcich pravidiel;
- U. keďže vo svojom stanovisku z 5. decembra 2018 Európsky výbor pre ochranu údajov na základe dokumentácie predloženej Komisiou posudzuje, či japonský právny rámec pre ochranu údajov poskytuje jednotlivcom dostatočné záruky primeranej úrovne ochrany údajov; keďže Európsky výbor pre ochranu údajov víta úsilie Komisie a japonskej komisie PPC o zvýšenie konvergencie medzi japonským a európskym právnym rámcom s cieľom uľahčiť prenos osobných údajov; keďže Európsky výbor pre ochranu údajov uznáva, že zlepšenia, ktorými sa zaviedli dodatočné pravidlá na preklopenie niektorých rozdielov medzi týmito dvoma rámcami, sú veľmi dôležité a pozitívne prijaté; keďže konštatuje, že pretrvávajú viaceré obavy, napr. v súvislosti s ochranou osobných údajov prenášaných z EÚ do Japonska počas celého ich životného cyklu, a odporúča Komisii, aby poskytla ďalšie dôkazy a vysvetlenia týkajúce sa nastolených problémov a podrobne monitorovala účinné uplatňovanie týchto pravidiel;
- V. keďže návrh vykonávacieho rozhodnutia je doplnený aj listom ministra spravodlivosti zo 14. septembra 2018, v ktorom odkazuje na dokument, ktorý vypracovalo ministerstvo spravodlivosti a viaceré ministerstvá a agentúry, s názvom Zhromažďovanie a používanie osobných informácií japonskými orgánmi verejnej moci na účely presadzovania trestného práva a národnej bezpečnosti, ktorý obsahuje prehľad platného právneho rámca a Komisii poskytuje úradné vyhlásenia, záruky a záväzky podpísané na najvyššej úrovni ministrov a agentúr a ktorý je pripojený ako príloha II k vykonávaciemu rozhodnutiu;
1. berie na vedomie podrobnú analýzu, ktorú Komisia poskytla vo svojom návrhu vykonávacieho rozhodnutia o primeranosti v súvislosti so zárukami vrátane mechanizmov dohľadu a nápravy, ktoré sa vzťahujú na spracovanie údajov komerčnými subjektmi, ako aj na prístup japonských verejných orgánov k údajom, najmä v oblasti presadzovania práva a národnej bezpečnosti;
 2. berie na vedomie skutočnosť, že Japonsko zároveň pripravuje aj uznanie úrovne ochrany osobných údajov prenášaných z Japonska do EÚ podľa článku 23 APPI, výsledkom čoho by bolo vôbec prvé „vzájomné“ zistenie o primeranosti na celom svete a viedlo by to k vytvoreniu najväčšej oblasti voľného a bezpečného toku údajov na svete;
 3. víta tento vývoj ako prejav globálneho šírenia vysokých noriem v oblasti ochrany údajov; poukazuje však na to, že v rozhodnutiach EÚ o primeranosti to nesmie v

žiadnom prípade viesť k prístupu „oko za oko, zub za zub“; pripomína, že v súvislosti s rozhodnutím o primeranosti podľa všeobecného nariadenia o ochrane údajov musí Komisia objektívne posúdiť právnu a praktickú situáciu v tretej krajine, na území, v sektore alebo medzinárodnej organizácii;

4. poukazuje na to, že Súdny dvor EÚ rozhodol, že výraz „primeraná úroveň ochrany“ si nevyžaduje úroveň ochrany identickú s úrovňou ochrany zaručenou v rámci EÚ, pričom ho „však treba chápať v tom zmysle, že vyžaduje, aby táto tretia krajina skutočne zaistila z dôvodu jej vnútroštátneho práva alebo medzinárodných dohôd, ktoré podpísala, úroveň ochrany slobôd a základných práv, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie podľa všeobecného nariadenia o ochrane údajov v spojení s Chartou“;
5. poznamenáva, že právo na súkromie a ochranu osobných údajov je na ústavnej úrovni zaručené v Japonsku aj v EÚ, ale úplné zosúladenie pravidiel EÚ a Japonska nebude možné vzhľadom na rozdiely v ústavnej štruktúre, ako aj v kultúre;
6. berie na vedomie zmeny APPI, ktoré nadobudli účinnosť 30. mája 2017; víta podstatné zlepšenia;
7. konštatuje, že kategórie obchodných a spracovateľských činností, ktoré sú vylúčené z vecnej pôsobnosti APPI, boli výslovne vylúčené z pôsobnosti zistenia o primeranosti;
8. domnieva sa, že po prijatí zmien APPI a všeobecného nariadenia o ochrane údajov v roku 2016 majú japonské systémy a systémy EÚ na ochranu údajov vysoký stupeň konvergencie, pokiaľ ide o zásady, záruky a individuálne práva, ako aj mechanizmy dohľadu a presadzovania; zdôrazňuje najmä vytvorenie nezávislého dozorného orgánu – komisie PPC, prostredníctvom zmeneného APPI;
9. konštatuje však, že samotná PPC sa domnieva, že „napriek vysokému stupňu konvergencie medzi týmito dvoma systémami existujú určité relevantné rozdiely“; takisto poznamenáva, že na zabezpečenie vyššej úrovne ochrany osobných údajov prenášaných z EÚ prijala komisia PPC 15. júna 2018 doplňujúce pravidlá;
10. víta niekoľko dôležitých objasnení v doplňujúcich pravidlách vrátane zosúladenia anonymizovaných osobných údajov v zákone APPI s vymedzením pojmu „anonymné informácie“ vo všeobecnom nariadení o ochrane údajov;
11. domnieva sa, že dodatočná ochrana doplňujúcich pravidiel sa vzťahuje len na prenosi na základe rozhodnutí o primeranosti; pripomína, že vzhľadom na rozsah rozhodnutia o primeranosti sa niektoré prenosi údajov uskutočnia podľa týchto iných dostupných mechanizmov;
12. uznáva, že dodatočná ochrana ustanovená v doplňujúcich pravidlách sa obmedzuje len na osobné údaje prenášané z Európy, a preto podnikateľské subjekty, ktoré musia súčasne spracúvať japonské aj európske osobné údaje, budú povinné dodržiavať doplňujúce pravidlá, napr. tak, že zabezpečia technické opatrenia („štítky“) alebo organizačné opatrenia (napr. uloženie do vyhradenej databázy), aby bolo možné takéto osobné údaje identifikovať počas celého ich životného cyklu; vyzýva Komisiu, aby situáciu monitorovala s cieľom predísť prípadným medzerám, ktoré by podnikateľským subjektom umožnili obchádzať povinnosti stanovené v doplňujúcich pravidlách tým, že

údaje prenesú prostredníctvom tretích krajín;

13. konštatuje, že vymedzenie pojmu „osobné údaje“ v APPI vylučuje údaje „definované vládny nariadením ako údaje, v súvislosti s ktorými existuje malá možnosť poškodenia práv a záujmov jednotlivca s ohľadom na metódu ich používania“; naliehavo vyzýva Komisiu, aby posúdila, či je tento prístup, ktorý je založený na možnosti poškodenia, v súlade s prístupom EÚ, v rámci ktorého patrí každé spracovanie osobných údajov do rozsahu pôsobnosti právnych predpisov o ochrane údajov; konštatuje však zároveň, že tento prístup by sa uplatňoval len vo veľmi obmedzených prípadoch;
14. ďalej konštatuje, že vymedzenie pojmu „osobné informácie“ v APPI je obmedzené na informácie, „podľa ktorých možno identifikovať konkrétnu osobu“; ďalej poznamenáva, že toto vymedzenie nezahŕňa objasnenie poskytnuté vo všeobecnom nariadení o ochrane údajov, podľa ktorého by sa mali za osobné údaje taktiež považovať osobné informácie, keď ich možno použiť len na osobitný výber jednej osoby, ako je jasne stanovené Súdnym dvorom EÚ;
15. vyjadruje znepokojenie nad tým, že užšie vymedzenie pojmu „osobné údaje“ (na základe vymedzenia pojmu „osobné informácie“) v APPI nemusí spĺňať normu byť „v podstate rovnocenná“ s ohľadom na všeobecné nariadenie o ochrane údajov a judikatúru Súdneho dvora; spochybňuje preto vyhlásenie v návrhu vykonávacieho rozhodnutia o tom, že „údaje EÚ budú vždy patriť do kategórie „osobných údajov“ v rámci APPI“; vyzýva Komisiu, aby pozorne monitorovala praktické dôsledky rôznych koncepcií v priebehu uplatňovania rozhodnutia o primeranosti a jeho pravidelného preskúmania;
16. vyzýva Komisiu, aby poskytla ďalšie objasnenia a v prípade potreby od japonských orgánov požadovala ďalšie záväzné doplňujúce pravidlá s cieľom zabezpečiť, aby všetky osobné údaje v zmysle všeobecného nariadenia o ochrane údajov boli pri svojom prenose do Japonska chránené;
17. so znepokojením konštatuje, že odlišne od právnych predpisov EÚ neobsahujú APPI ani usmernenia komisie PPC právne ustanovenia týkajúce sa automatizovaného rozhodovania a profilovania a že túto otázku riešia len niektoré sektorové pravidlá, a to bez toho, aby poskytovali komplexný celkový právny rámec so značnou a silnou ochranou pred automatizovaným rozhodovaním a profilovaním; vyzýva Komisiu, aby preukázala, ako sa táto otázka rieši v rámci japonského rámca na ochranu údajov, a to takým spôsobom, aby sa zabezpečila rovnaká úroveň ochrany; domnieva sa, že je to relevantné najmä vzhľadom na nedávne prípady profilovania Facebook/Cambridge Analytica;
18. domnieva sa, že na základe referenčného kritéria primeranosti Európskeho výboru pre ochranu údajov sú potrebné ďalšie podrobné objasnenia v oblasti priameho marketingu vzhľadom na to, že v APPI neexistujú žiadne osobitné ustanovenia, a to s cieľom preukázať rovnocennú úroveň ochrany osobných údajov v Japonsku;
19. berie na vedomie stanovisko Európskeho výboru pre ochranu údajov, v ktorom sa uvádza niekoľko problematických oblastí, napr. ochrana osobných údajov prenášaných z EÚ do Japonska počas celého ich životného cyklu; vyzýva Komisiu, aby venovala vykonávaciemu rozhodnutiu primeranú pozornosť a poskytla v ňom ďalšie dôkazy a vysvetlenia preukazujúce existenciu primeraných záruk;

20. vyzýva Komisiu, aby objasnila, či pokiaľ ide o následné prenosy, riešenie stanovené v doplnujúcich pravidlách, ktoré spočíva v požiadavke predchádzajúceho súhlasu dotknutých osôb z EÚ so schválením následného prenosu tretej strane v cudzej krajine, neobsahuje určité podstatné prvky, ktoré by dotknutým osobám umožnili vyjadriť svoj súhlas, pretože výslovne nedefinuje, čo zahŕňa pojem „informácie o okolnostiach prenosu, ktoré sú pre [dotknutú osobu] nevyhnutné na prijatie rozhodnutia o svojom súhlase“, v súlade s článkom 13 všeobecného nariadenia o ochrane údajov, napr. v súvislosti s treťou krajinou určenia následného prenosu; vyzýva Komisiu, aby ďalej objasnila dôsledky vyplývajúce pre dotknutú osobu v prípade odmietnutia súhlasu s následným prenosom jej osobných údajov;
21. vyjadruje poľutovanie nad tým, že pokiaľ ide o účinné presadzovanie APPI, nie je výška prípadných pokút, ktoré by uložili trestné orgány, dostatočná na zabezpečenie účinného súladu so zákonom, keďže sa nezdá, že by bola vo vzťahu k závažnosti porušenia primeraná, účinná ani odrádzajúca; konštatuje však, že v APPI sa stanovujú aj trestné sankcie vrátane trestu odňatia slobody; vyzýva Komisiu, aby poskytla informácie o skutočnom využívaní správnych pokút a trestných sankcií v minulosti;
22. berie na vedomie, že hoci komisia PPC nemá žiadny dohľad nad činnosťami spracúvania údajov v oblasti presadzovania práva, existujú iné mechanizmy dohľadu vrátane dohľadu zo strany nezávislej komisie pre verejnú bezpečnosť v rámci prefektúr; konštatuje, že Rada pre preskúvanie zverejňovania informácií a ochrany osobných údajov má v tejto oblasti taktiež určité právomoci vrátane preskúmania žiadostí o prístup a zverejňovania stanovísk, ale poukazuje na to, že tieto právomoci nie sú právne záväzné; víta skutočnosť, že EÚ a Japonsko sa dohodli, že zavedú osobitný mechanizmus nápravy, ktorý bude riadený komisiou PPC a pod jej dohľadom a ktorý sa bude vzťahovať na spracovanie osobných údajov v oblasti presadzovania práva a bezpečnosti štátu;
23. konštatuje, že podľa japonského zákona o ochrane osobných informácií uchovávaných správnymi orgánmi (APPIHAO) môžu podnikateľské subjekty poskytovať údaje orgánom presadzovania práva aj na „dobrovoľnom základe“; poukazuje na to, že to nie je stanovené vo všeobecnom nariadení o ochrane údajov ani v tzv. policajnej smernici, a vyzýva Komisiu, aby posúdila, či je to v súlade s normou byť „v podstate rovnocenná“ k všeobecnému nariadeniu o ochrane údajov;
24. je si vedomý mediálnych správ o japonskom riaditeľstve pre získavanie spravodajských informácií zachytávaním signálov (DFS), „ktoré zamestnáva približne 1 700 ľudí a má aspoň šesť sledovacích zariadení na neustále odpočúvanie a sledovanie telefonických hovorov, e-mailov a iných komunikačných kanálov“¹; vyjadruje znepokojenie nad tým, že tento prvok plošného hromadného sledovania sa v návrhu vykonávacieho rozhodnutia vôbec nespomína; vyzýva Komisiu, aby poskytla viac informácií o japonskom hromadnom sledovaní; vyjadruje vážne znepokojenie nad tým, že toto hromadné sledovanie neobstojí v skúške kritériami, ktoré stanovil Súdny dvor EÚ v rozsudku Schrems (vec C-362/14);
25. vyjadruje poľutovanie nad tým, že dokument s názvom Zhromažďovanie a využívanie

¹ Ryan Gallagher, Neznámy príbeh japonskej tajnej špionážnej služby (The Untold Story of Japan's Secret Spy Agency), The Intercept, 19. máj 2018, <https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/>

osobných informácií japonskými orgánmi verejnej moci na účely presadzovania trestného práva a národnej bezpečnosti, ktorý je súčasťou prílohy II k návrhu vykonávacieho rozhodnutia, nemá rovnaký právne záväzný účinok ako doplňujúce pravidlá;

Závery

26. vyzýva Komisiu, aby poskytla ďalšie dôkazy a vysvetlenia týkajúce sa uvedených záležitostí vrátane tých, ktoré identifikoval Európsky výbor pre ochranu údajov vo svojom stanovisku z 5. decembra 2018, s cieľom preukázať, že japonský právny rámec na ochranu údajov zabezpečuje primeranú úroveň ochrany, ktorá je v podstate rovnocenná ochrane poskytovanej európskym právnym rámcom na ochranu údajov;
27. domnieva sa, že toto rozhodnutie o primeranosti môže okrem toho vyslať jasný signál krajinám na celom svete, že konvergencia s prísnyimi normami EÚ v oblasti ochrany údajov prináša veľmi konkrétne výsledky; v tejto súvislosti zdôrazňuje význam tohto rozhodnutia o primeranosti ako precedensu pre budúce partnerstvá s ďalšími krajinami, ktoré prijali moderné právne predpisy na ochranu údajov;
28. poveruje Výbor pre občianske slobody, spravodlivosť a vnútorné veci, aby naďalej sledoval vývoj v tejto oblasti, a to aj v prípadoch predložených Súdnemu dvoru, a monitoroval následné opatrenia prijímané v nadväznosti na odporúčania uvedené v tomto uznesení;

o

o o

29. poveruje svojho predsedu, aby postúpil toto uznesenie Rade, Komisii, vládam a parlamentom členských štátov, Európskemu výboru pre ochranu údajov, európskemu dozornému úradníkovi pre ochranu údajov, výboru zriadenému podľa článku 93 ods. 1 všeobecného nariadenia o ochrane údajov, Rade Európy a vláde Japonska.