Okvir za varstvo zasebnosti podatkov med EU in ZDA

POGOSTO POSTAVLJENA VPRAŠANJA ZA EVROPSKA PODJETJA[1]

Sprejeto 16. julija 2024

[1] V tem okviru evropska podjetja pomenijo podjetja v EGP, ki prenašajo ali bi lahko prenašala osebne podatke podjetjem v ZDA, potrjenim v sklopu okvira za varstvo zasebnosti podatkov.

Sprejeto

Kazalo

VPRAŠANJE 1 Kaj je okvir za varstvo zasebnosti podatkov med EU in ZDA?.....3

VPRAŠANJE 2 Katera podjetja iz ZDA lahko uporabljajo okvir za varstvo zasebnosti podatkov med EU in ZDA?.....3

VPRAŠANJE 3 Kaj je treba storiti pred prenosom osebnih podatkov podjetju iz ZDA, ki je ali naj bi bilo certificirano v sklopu okvira za varstvo zasebnosti podatkov med EU in ZDA?.....4

VPRAŠANJE 4 Kje lahko najdem smernice v zvezi s certificiranjem ameriških hčerinskih družb evropskih podjetij?.....6

VPRAŠANJE 1 – KAJ JE OKVIR ZA VARSTVO ZASEBNOSTI PODATKOV MED EU IN ZDA?

Okvir za varstvo zasebnosti podatkov med EU in ZDA je mehanizem samocertificiranja podjetij iz ZDA. Podjetja, ki so se samocertificirala v sklopu okvira za varstvo zasebnosti podatkov, morajo upoštevati njegova načela, pravila in obveznosti v zvezi z obdelavo osebnih podatkov posameznikov iz EGP. Za več informacij o teh zavezah glejte načela okvira za varstvo zasebnosti podatkov.[2]

Evropska komisija je ugotovila, da so prenosi osebnih podatkov iz EGP podjetjem v ZDA, ki so certificirana v sklopu okvira za varstvo zasebnosti podatkov, ustrezno zaščiteni.[3] Zato se lahko osebni podatki certificiranim podjetjem iz ZDA prenesejo, ne da bi bilo treba vzpostaviti dodatne zaščitne ukrepe ali pridobiti kakršno koli dovoljenje. V nadaljevanju je navedenih nekaj koristnih povezav, na katerih najdete več informacij.

- Vprašanja in odgovori Evropske komisije: okvir za varstvo zasebnosti podatkov[4]
- Spletno mesto o okviru za varstvo zasebnosti podatkov, ki ga upravlja ameriško Ministrstvo za trgovino[5]
- Sklep Evropske komisije o ustrezni ravni varstva osebnih podatkov v skladu z okvirom za varstvo zasebnosti podatkov med EU in ZDA[6]

Okvir za varstvo zasebnosti podatkov se uporablja za vse vrste osebnih podatkov, ki se prenašajo iz EGP v ZDA, vključno z osebnimi podatki, ki se obdelujejo za komercialne ali zdravstvene namene, in podatki o človeških virih, zbranimi v okviru delovnega razmerja (v nadaljevanju: „podatki o človeških virih“), kadar je podjetje iz ZDA, ki je prejemnik podatkov, samocertificirano za obdelavo tovrstnih podatkov na podlagi okvira za varstvo zasebnosti podatkov.[7]

VPRAŠANJE 2 – KATERA PODJETJA IZ ZDA LAHKO UPORABLJAJO OKVIR ZA VARSTVO ZASEBNOSTI PODATKOV MED EU IN ZDA?

Da bi se podjetje iz ZDA lahko kvalificiralo za samocertificiranje v sklopu okvira za varstvo zasebnosti podatkov, mora biti podvrženo preiskovalnim in izvršilnim pooblastilom ameriške Zvezne komisije za

---

[2] https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles

[3] Evropska komisija je 10. julija 2023 sprejela sklep o ustreznosti okvira za varstvo zasebnosti podatkov med EU in ZDA. Okvir sta skupaj zasnovala Evropska komisija in ameriško Ministrstvo za trgovino, da bi nadomestila Sklep o zasebnostnem ščitu (EU) 2016/1250, ki ga je Sodišče Evropskih skupnosti 16. julija 2020 v zadevi C-311/18 *Data Protection Commissioner/Facebook Ireland Limited in Maximillian Schrems (zadeva Schrems II),* razglasilo za neveljavnega.

[4] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[5] https://www.dataprivacyframework.gov/s/

[6] https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

[7] Upoštevati je treba, da podatki o človeških virih niso zajeti v vseh primerih samocertificiranja v sklopu okvira za varstvo zasebnosti podatkov. Zato je pomembno preveriti, ali to velja tudi v posameznem primeru, če je ustrezno. Glejte tudi 3. vprašanje.

trgovino (FTC) ali Ministrstva za promet (DoT). V prihodnosti bodo morda vključeni tudi drugi ameriški zakonsko določeni organi.[8]

To pomeni, da se na primer nepridobitne organizacije, banke, zavarovalnice in ponudniki telekomunikacijskih storitev (v zvezi z dejavnostmi skupnih operaterjev), ki ne spadajo med pristojnosti zvezne Komisije za trgovino ali Ministrstva za promet, ne morejo samocertificirati v sklopu okvira za varstvo zasebnosti podatkov.

VPRAŠANJE 3 – KAJ JE TREBA STORITI PRED PRENOSOM OSEBNIH PODATKOV PODJETJU IZ ZDA, KI JE ALI NAJ BI BILO CERTIFICIRANO V SKLOPU OKVIRA ZA VARSTVO ZASEBNOSTI PODATKOV MED EU IN ZDA?

Pred prenosom osebnih podatkov podjetju iz ZDA, ki trdi, da je samocertificirano v sklopu okvira za varstvo zasebnosti podatkov, mora izvoznik podatkov v EGP preveriti, ali ima podjetje iz ZDA aktiven samocertifikat (certifikate je treba vsako leto podaljšati) in ali ta certifikat zajema zadevne podatke (zlasti če zajema podatke o človeških virih oziroma druge podatke).[9]

Da bi preverili, ali je samocertifikat aktiven in veljaven, morajo izvozniki podatkov v EGP preveriti, ali je podjetje iz ZDA navedeno na seznamu okvira za varstvo zasebnosti podatkov,[10] objavljenem na spletnem mestu ministrstva za trgovino ZDA. Ta seznam vključuje tudi register podjetij, ki so bila odstranjena s seznama („neaktivni udeleženci“), z navedbo razlogov za odstranitev. Izvoznik podatkov iz EGP se pri prenosih osebnih podatkov v tovrstna podjetja ne more sklicevati na okvir za varstvo zasebnosti podatkov. Upoštevajte, da morajo podjetja, ki so bila odstranjena s seznama okvira za varstvo zasebnosti podatkov, še naprej upoštevati načela okvira za varstvo zasebnosti podatkov pri osebnih podatkih, ki jih prejmejo med sodelovanjem v okviru za varstvo zasebnosti podatkov, dokler te hranijo.

Za prenos osebnih podatkov podjetjem iz ZDA, ki niso (ali niso več) samocertificirana v sklopu okvira za varstvo zasebnosti podatkov, se lahko uporabijo drugi razlogi za prenos iz poglavja V Splošne uredbe o varstvu podatkov, kot so zavezujoča poslovna pravila ali standardna pogodbena določila.

Dejstvo, da je uporabnik iz ZDA samocertificiran v sklopu okvira za varstvo zasebnosti podatkov, bo izvoznikom podatkov iz EGP omogočilo skladnost s poglavjem V Splošne uredbe o varstvu podatkov, vendar se še naprej uporabljajo vse druge zahteve iz navedene uredbe in katere koli druge nacionalne zakonodaje o varstvu podatkov.

3.1. Prenosi hčerinskim družbam iz ZDA, ki so certificirane v sklopu okvira za varstvo zasebnosti podatkov med EU in ZDA.

[8] Glejte Prilogo I k sklepu o ustreznosti, načela okvira za varstvo zasebnosti podatkov med EU in ZDA, ki jih je izdalo Ministrstvo za trgovino ZDA, odstavek I.2.

[9] Glejte opredelitev podatkov o človeških virih pri 1. vprašanju.

[10] https://www.dataprivacyframework.gov/list

V primeru prenosov podatkov podjetjem iz ZDA, ki so hčerinske družbe matičnega podjetja, certificiranega v sklopu okvira za varstvo zasebnosti podatkov, morajo izvozniki podatkov iz EGP preveriti, ali certifikat matičnega podjetja zajema tudi zadevno hčerinsko družbo.

Dodatne informacije o tem, kako preveriti obseg samocertifikacije organizacije, vključno s tem, ali so v njej zajeti tudi drugi ameriški subjekti ali podružnice iz ZDA, najdete tukaj.[11]

3.2. Prenosi podjetju iz ZDA, ki deluje kot upravljavec

Pred prenosom osebnih podatkov upravljavcu iz ZDA mora izvoznik podatkov iz EGP zagotoviti, da je prenos v skladu z vsemi ustreznimi določbami Splošne uredbe o varstvu podatkov. Kot prvi korak sme izvoznik podatkov osebne podatke deliti s podjetjem iz ZDA le, če obstaja pravna podlaga za obdelavo (6. člen Splošne uredbe o varstvu podatkov). Poleg tega morajo biti izpolnjene vse druge zahteve iz Splošne uredbe o varstvu podatkov (na primer omejitev namena, sorazmernost, točnost in obveznosti glede obveščanja posameznikov). Upoštevajte, da mora izvoznik podatkov iz EGP pri prenosu podatkov samocertificiranemu podjetju iz ZDA v skladu s 13. in 14. členom Splošne uredbe o varstvu podatkov posameznike obvestiti o identiteti prejemnikov njihovih podatkov in o dejstvu, da je prenos zajet s sklepom o ustreznosti okvira za varstvo zasebnosti podatkov med EU in ZDA.

3.3. Prenosi podjetju iz ZDA, ki deluje kot obdelovalec

Kadar upravljavec iz EGP prenese podatke obdelovalcu iz ZDA, morata upravljavec in obdelovalec skleniti sporazum o obdelavi podatkov v skladu z 28. členom Splošne uredbe o varstvu podatkov (v nadaljevanju: sporazum o obdelavi podatkov), ne glede na to, ali je obdelovalec samocertificiran v sklopu okvira za varstvo zasebnosti podatkov.

Več informacij o pogodbenih zahtevah za prenose obdelovalcu iz ZDA najdete tukaj.[12]

Sklenitev sporazuma o obdelavi podatkov je potrebna za zagotovitev, da se obdelovalec iz ZDA zaveže, da:

- osebne podatke obdeluje samo po dokumentiranih navodilih upravljavca, vključno glede prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo, razen če to od njega zahteva pravo Unije ali države članice, ki velja za obdelovalca; v slednjem primeru obdelovalec o tej pravni zahtevi pred obdelavo podatkov obvesti upravljavca, razen če zadevno pravo prepoveduje takšno obvestilo na podlagi pomembnih razlogov v javnem interesu;
- zagotovi, da so osebe, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon;
- uvede ustrezne tehnične in organizacijske ukrepe za zagotovitev ravni varnosti, ki ustreza tveganju, v skladu s tem, kar se zahteva v sporazumu o obdelavi podatkov (na podlagi 32. člena Splošne uredbe o varstvu podatkov) ter 4. in 10. oddelku okvira za varstvo zasebnosti podatkov;

[11] https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-(DPF)-Commitments

[12] https://www.dataprivacyframework.gov/program-articles/Contract-Requirements-for-Data-Transfers-to-a-Processor

- spoštuje pogoje, navedene v pogodbi o obdelavi podatkov (ki izhajajo iz drugega in četrtega odstavka 28. člena Splošne uredbe o varstvu podatkov) in II.3.B oddelka okvira za varstvo zasebnosti podatkov, pri vključitvi drugega obdelovalca;
- ob upoštevanju narave obdelave pomaga upravljavcu z ustreznimi tehničnimi in organizacijskimi ukrepi, kolikor je to mogoče, pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika iz III. poglavja Splošne uredbe o varstvu podatkov;
- upravljavcu pomaga pri izpolnjevanju obveznosti iz 32. do 36. člena Splošne uredbe o varstvu podatkov ob upoštevanju narave obdelave in informacij, ki so dostopne obdelovalcu;
- v skladu z odločitvijo upravljavca izbriše ali vrne vse osebne podatke upravljavcu po zaključku storitev v zvezi z obdelavo ter uniči obstoječe kopije, razen če pravo Unije ali pravo države članice predpisuje shranjevanje osebnih podatkov;
- upravljavcu da na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz 28. člena Splošne uredbe o varstvu podatkov, ter upravljavcu ali drugemu revizorju, ki ga pooblasti upravljavec, omogoči izvajanje revizij, tudi pregledov, in pri njih sodeluje. V zvezi s to zadnjo točko obdelovalec nemudoma obvesti upravljavca, če po njegovem mnenju navodilo krši okvir za varstvo zasebnosti podatkov.

Kadar obdelovalec iz ZDA najame drugega obdelovalca („podobdelovalca“) za izvajanje posebnih dejavnosti obdelave v imenu upravljavca iz EGP, mora obdelovalec zagotoviti, da so izpolnjene zahteve iz II.3.B oddelka okvira za varstvo zasebnosti podatkov. To vključuje zagotavljanje, da podobdelovalec zagotavlja enako raven varstva osebnih podatkov, kot se zahteva v okviru za varstvo zasebnosti podatkov, in enake obveznosti glede varstva podatkov, kot so določene v pogodbi o obdelavi podatkov. Kadar podobdelovalec ne izpolni obveznosti varstva podatkov, prvi obdelovalec iz ZDA še naprej v celoti odgovarja upravljavcu za izpolnjevanje obveznosti navedenega podobdelovalca.

VPRAŠANJE 4 – KJE LAHKO NAJDEM SMERNICE V ZVEZI S CERTIFICIRANJEM AMERIŠKIH HČERINSKIH DRUŽB EVROPSKIH PODJETIJ?

Ameriške hčerinske družbe podjetij iz EGP se lahko samocertificirajo v sklopu okvira za varstvo zasebnosti podatkov, če so v pristojnosti ameriške Zvezne komisije za trgovino (FTC) ali Ministrstva za promet (DoT).

Več informacij o zahtevah glede upravičenosti lahko najdete tukaj,[13] navodila za postopek samocertificiranja pa tukaj.[14]

[13] https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-(DPF)-Program

[14] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931)