Pravila GDPR se uporabljajo tudi izven ozemlja EU za urejanje prenosa osebnih podatkov, ki ga gospodarski subjekt s sedežem v državi članici EU v komercialne namene izvede drugemu gospodarskemu subjektu s sedežem v tretji državi.

Regulativa

Prekomejni prenosi osebnih podatkov med EU in ZDA – ali bodo še mogoči?

Splošna uredba o varstvu podatkov (GDPR) je poleg enotnih pravil za varstvo osebnih podatkov v EU postavila tudi pravila za morebiten prenos teh podatkov v tretje države. Po odmevni razveljavitvi »zasebnostnega ščita« v letu 2020, ki je pred tem omogočal prenos podatkov iz EU v ZDA, je ta skladno s pravili GDPR mogoč na drugih pravnih podlagah – predvsem na podlagi standardnih pogodbenih klavzul.

Špela Ajdišek Robič, vodja pravne službe pri Siemens d.o.o.

Špela Ajdišek Robič

Pred spremembo ureditve prava zasebnosti v EU, ki jo je spodbudilo Sodišče EU, se je zgodilo kar nekaj odmevnih primerov, ki so kazali na različnost ureditve varstva zasebnosti po svetu.

Splošna uredba o varstvu podatkov (Uredba (EU) 2016/679 – GDPR) je poleg enotnih pravil za varstvo osebnih podatkov v Evropski uniji postavila tudi pravila za morebiten prenos teh podatkov v države izven EU, torej v tretje države. Pravila GDPR se tako uporabljajo tudi izven ozemlja EU za urejanje prenosa osebnih podatkov, ki ga gospodarski subjekt s sedežem v državi članici EU v komercialne namene izvede drugemu gospodarskemu subjektu s sedežem v tretji državi. Ta je po GDPR dovoljen, če država prejemnica teh podatkov preko svoje domače zakonodaje ali mednarodnih obveznosti zagotavlja takšno raven varstva osebnih podatkov, ki je ustrezna in enakovredna ravni varstva, zagotovljenega v EU na podlagi GDPR. Pristojnost za ugotovitev ustreznosti varstva ima po GDPR Evropska komisija, ki o tem odloči s sklepom (kakršna je bila odločba o varnem pristanu iz leta 2000 ali o zasebnostnem ščitu iz leta 2016). Če ta ugotovi, da ustreznosti varstva v tretji državi ni, je prenos osebnih podatkov v to državo mogoč le, če gospodarski subjekt s sedežem v EU kot izvoznik osebnih podatkov predvidi ustrezne zaščitne ukrepe in če imajo posamezniki, čigar osebni podatki se obdelujejo, na voljo učinkovita pravna sredstva ter izvršljive pravice za uveljavitev tega varstva.

Odmevni primeri in razlike v ureditvi varstva zasebnosti po svetu

Pred spremembo ureditve prava zasebnosti v EU, ki jo je spodbudilo Sodišče EU, se je zgodilo kar nekaj odmevnih primerov, ki so kazali na različnost ureditve varstva zasebnosti po svetu.

Edward Joseph Snowden je v vlogi »žvižgača« junija 2013 razkril informacije o ameriškem nadzorovanju telefonskih in spletnih informacij v ZDA in tujini ter objavil strogo zaupne dokumente programov Ameriške agencije za nacionalno varnost (NSA), kamor sodi tudi t. i. nadzorni program PRISM za zbiranje in analizo velikih količin osebnih podatkov o posameznikih. Istega leta je avstrijski državljan Maximilian Schrems pri irskem nadzornem organu za varstvo osebnih podatkov zahteval prepoved prenosa njegovih osebnih podatkov, pridobljenih s strani družbe Facebook Irska, na strežnike v lasti družbe Facebook Inc., saj naj ZDA ne bi zagotavljale zadostnega varstva osebnih podatkov posameznikov, ki so bili preneseni v posamezno zvezno državo, pred dostopom ameriških državnih organov do teh podatkov. Problematični so bili predvsem dostopi s strani NSA v okviru prej omenjenega programa PRISM. Njegova pritožba je bila sicer s strani irskega organa zavrnjena (tudi iz razloga, ker je Evropska komisija v tako imenovani Odločbi o »varnem pristanu« ugoto-

vila ustrezno raven varstva osebnih podatkov s strani ZDA), vendar pa je v končni posledici vendarle sprožila odločanje Sodišča EU o ustreznosti varstva podatkov.

Najprej razveljavitev »varnega pristana« ...

Sodišče EU je leta 2015 odločbo Komisije o »varnem pristanu« razglasilo za neveljavno (sodba Schrems I). Med razlogi je Sodišče navedlo prav omejitve v zvezi z dostopom javnih organov ZDA do prenesenih podatkov in odsotnost učinkovitega pravnega varstva pred takim vpogledom in dostopom javnih organov. Po mnenju Sodišča EU zakonodaja, ki na splošni podlagi dovoljuje dostop javnih organov do vsebine elektronskih komunikacij in podobnih osebnih podatkov, ogroža temeljne pravice do spoštovanja zasebnega življenja. Da bi zadostili potrebam poslovne skupnosti na obeh straneh Atlantika, sta EU in ZDA po razveljavitvi dogovora o »varnem pristanu« sklenili nov dogovor o izmenjavi podatkov – Sporazum o »zasebnostnem ščitu«, katerega ustreznost z vidika varstva podatkov je Evropska komisija potrdila s sklepom 2016/1250. S tem pa je bil zopet zagotovljen mehanizem za čezatlantske prenose podatkov, na osnovi katerega so se podjetja »samocertificirala«.

... nato pa tudi »zasebnostnega ščita«

Na osnovi prenovljene pritožbe Maximiliana Schremsa, ki je upoštevala sodno prakso »Schrems I«, je irski nadzorni organ za varstvo osebnih podatkov vprašanje prenosa podatkov iz EU v ZDA v njegovem primeru zopet postavil pred sodišče EU. To je v odmevni sodbi, imenovani »Schrems II«, razveljavilo tudi sklep št. 2016/1250. Schrems II pomeni sodbo, s katero je bil »zasebnostni ščit« razglašen za neveljavno pravno podlago za prenos osebnih podatkov med EU in ZDA. Sodišče je odločitev utemeljilo z navedbo, da varstvo osebnih podatkov, kot ga zagotavlja zakonodaja v ZDA, ni enakovredno ravni varstva v EU. S tem v zvezi je izpostavilo predvsem preširoka pooblastila organov javne varnosti, obrambe in državne varnosti pri dostopu do prenesenih osebnih podatkov ter neustreznost pooblastil instituta ameriškega varuha človekovih pravic, ki bi moral zagotavljati učinkovito pravno varstvo.

Prenos osebnih podatkov na podlagi standardnih pogodbenih klavzul

Ne glede na to pa je Sodišče pustilo v veljavi sklep Evropske komisije št. 2010/87, s čimer dovoljuje prenos osebnih podatkov na podlagi standardnih pogodbenih klavzul. Po mnenju Sodišča EU te vsebujejo učinkovite mehanizme za prenos podatkov z adekvatno ravnjo varstva, ki ga zahteva pravo EU. Istočasno omogočajo, da se prenosi osebnih podatkov v primeru kršitve začasno ustavijo ali prepovejo. V zvezi z vprašanjem preširokih pooblastil državnih organov tretje države je Sodišče s tem izvozniku kot tudi prejemniku podatkov naložilo obveznost, da preverita, ali se v tretji državi zahtevana raven varstva osebnih podatkov spoštuje. V primeru, da prejemnik ustrezne ravni varstva ni zmožen zagotavljati, je zavezan o tem obvestiti izvoznika, ta pa mora začasno ustaviti prenos podatkov oziroma odstopiti od pogodbe.

Prenos osebnih podatkov je treba utemeljiti na veljavni podlagi

Od razveljavitve zasebnostnega ščita (sodba Schrems II) dalje je torej prenos osebnih podatkov v ZDA še vedno mogoč, saj je odpadla zgolj ena izmed pravnih podlag za prenos osebnih podatkov, predvidenih v GDPR. Pomembno je, da upravljavci (še posebej, če so podatke v ZDA prenašali na podlagi Sporazuma o zasebnostnem ščitu) poskrbijo za utemeljitev prenosa na eni izmed preostalih veljavnih podlag in sami zagotovijo, da so vzpostavljeni ustrezni zaščitni ukrepi za varovanje zasebnosti ter temeljnih pravic in svoboščin posameznikov. Te se lahko zagotovi na različne načine – s standardnimi pogodbenimi določili o varstvu podatkov med družbo izvoznico in družbo prejemnico, nadalje z akreditacijskimi in certifikacijskimi mehanizmi, ki potrjujejo ustreznost varstva, pa tudi z zavezujočimi poslovnimi pravili družbe ter kodeksi ravnanja družb, sprejetimi po ustreznem postopku, ki zagotavljajo ustrezno varstvo po GDPR ter so potrjeni s strani organa za varstvo osebnih podatkov.

Po mnenju Sodišča EU zakonodaja, ki na splošni podlagi dovoljuje dostop javnih organov do vsebine elektronskih komunikacij in podobnih osebnih podatkov, ogroža temeljne pravice do spoštovanja zasebnega življenja.

Evropska komisija je urejanje pogodbenih razmerij glede prenosa podatkov olajšala in junija letos objavila nove standardne pogodbene klavzule (Uradni list EU L 199) – začele so veljati 27. junija 2021, ki služijo kot podlaga za prenos osebnih podatkov v tretje države. Čas za prilagoditev je najkasneje do 27. decembra 2022.

Varstvo osebnih podatkov, kot ga zagotavlja zakonodaja v ZDA, ni enakovredno ravni varstva v EU.

Posodobljene standardne klavzule so v obliki modulov, kar pomeni, da vključujejo različne scenarije obdelave osebnih podatkov. Module pogodbeni stranki izbereta glede na vsakokratne okoliščine prenosa: EU upravljavec – ne-EU upravljavec, EU upravljavec – ne-EU obdelovalec, EU obdelovalec – ne-EU obdelovalec in EU obdelovalec – ne-EU upravljavec.

S tem nove klavzule ponujajo možnost ureditve več različnih pogodbenih odnosov, predvsem pa imajo dvojne vsebinske spremembe. Po eni strani take, ki krepijo pravice posameznikov v odnosu do obdelovalcev, tako da jim omogočajo, da so obveščeni o postopkih obdelave njihovih podatkov, da imajo možnost, da vzpostavijo stik s tujimi upravljavci, da prejmejo kopijo sklenjenih klavzul, odškodnino za škodo v zvezi s kršitvami varstva osebnih podatkov in podobno. Po drugi strani pa take, ki krepijo položaj posameznika v odnosu do javnih organov, kot so pravno varstvo osebnih podatkov, uvedba omejitev pri razkrivanju osebnih podatkov javnim oblastem in določanje postopkov ocenjevanja in revizije, da se zagotovi skladnost s pogodbenimi klavzulami.

Dovoljen je prenos osebnih podatkov na podlagi standardnih pogodbenih klavzul, saj po mnenju Sodišča EU vsebujejo učinkovite mehanizme za prenos podatkov z adekvatno ravnjo varstva, ki ga zahteva pravo EU.

Standardne pogodbene klavzule so na nek način odgovornost za varstvo podatkov prenesle na izvoznika in uvoznika, ki s sklenitvijo le-teh jamčita, da nimata razloga za domnevo, da se izpolnjevanje obveznosti iz teh določil v namembni državi ne bi spoštovalo in podobno.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Gregor Krsmanović, direktor sektorja za splošne zadeve v A1 Slovenija

Prenos osebnih podatkov v ZDA je še vedno mogoč, pomembno pa je, da upravljavci poskrbijo za utemeljitev prenosa na eni izmed veljavnih podlag.

»V A1 Slovenija in skupini Telekom Austria Group je varstvo zasebnosti vgrajeno že v nabavni proces. S kar nekaj pogodbenimi partnerji, ki so sprva zavračali sklenitev pogodbenega razmerja z določenim zaščitnim ukrepom, torej s standardnimi pogodbenimi klavzulami, so bila potrebna dodatna usklajevanja pred sklenitvijo pogodbe. Skorajda v vseh primerih so se na trgu pojavile alternativne konkurenčne ponudbe evropskih podjetij, ki so izpolnjevale zahteve veljavnih predpisov.
Urejanje pogodbenih razmerij po razveljavitvi zasebnostnega ščita zahteva svoj čas in vztrajnost. Pomembno se je vprašati, s kom poslujemo in kakšnim tveganjem smo s tem izpostavljeni, ter ali so ta tveganja s kom drugim morda lahko drugačna. Vprašanje iznosa podatkov je postalo eno izmed bistvenih vprašanj, ki jih je treba urediti in doreči v začetku nabavnega procesa. Ne smemo pozabiti, da se enako sprašujejo tudi naši obstoječi in bodoči poslovni partnerji, ki jim prav tako ne bo več vseeno, s kom in kako imamo urejeno izmenjavo osebnih podatkov. Splošna uredba o varstvu podatkov (GDPR) je na eni strani prinesla kar nekaj izzivov, po drugi strani pa se izkazuje, da je osredotočenje na varstvo zasebnosti lahko pomembna konkurenčna prednost, kar je predvsem priložnost za podjetja iz EU, ki jo velja izkoristiti.«

Bor Juros, skrbnik informacijske varnosti v podjetju Xlab

Evropska komisija je urejanje pogodbenih razmerij glede prenosa podatkov olajšala in junija letos objavila nove standardne pogodbene klavzule (Uradni list EU L 199).

»V zadnjem času pri strankah, ki uporabljajo naš produkt ISL Online – ta uporabnikom omogoča dostop do oddaljenega računalnika oz. delo na daljavo –, opažamo porast vprašanj ter posledično tudi zahtev glede ravnanja s podatki. To pripisujemo večjemu zavedanju o pomenu zasebnosti ter porastu uporabe storitev za oddaljeni dostop do mobilnih naprav in računalnikov.
Zavezanost k informacijski varnosti strankam izkazujemo s certifikatom ISO 27001, z vidika omejevanja podatkovnih prenosov pa strankam ponujamo različne arhitekturne rešitve glede na njihove zahteve.
Zahtevnejšim strankam, katerih podatki ne smejo zapustiti območja EU, omogočamo postavitev zasebnega oblaka (Managed Private Cloud). Med postavitvijo postavimo strežnike na lokacijah po izbiri stranke, oblak pa je lahko dostopen navzven, ali pa je dosegljiv izključno v notranjem omrežju. Pri postavitvi MPC podatki nikoli ne zapustijo zasebnega oblaka, dostop do njih pa je omejen tudi našim tehnikom.«

Jaka Repanšek, vodja strateške skupine za regulativo, Slovenska digitalna koalicija

Standardne pogodbene klavzule so odgovornost za varstvo podatkov prenesle na izvoznika in uvoznika.

»Že dobro leto dni potekajo intenzivna usklajevanja med predstavniki Evropske unije in Združenih držav, ki bi privedla do novega krovnega sporazuma med EU in ZDA o prenosu podatkov. Kakršnakoli rešitev mora biti skladna z evropsko Uredbo o varstvu osebnih podatkov (GDPR) ter odločitvijo Sodišča EU v zadevah Schrems I in Schrems II, obenem pa je cilj, da bo nov dogovor omogočil enostavnejšo in preglednejšo izmenjavo in vpogled v osebne podatke med ZDA in EU.
Zlasti mala in srednja podjetja, pa tudi druge organizacije, ki v Sloveniji in številnih državah članicah EU tvorijo hrbtenico digitalnega ekosistema, vpetega v globalne informacijske tokove, si močno prizadevajo za čimprejšnjo sklenitev novega dogovora, saj za številna podjetja (zaradi pravne kompleksnosti ali zaradi poslovnih modelov digitalnega poslovanja in komuniciranja) uporaba standardnih pogodbenih določil ni dolgoročna (pravno, zlasti pa tehnično) ustrezna rešitev. Nujno je zbližanje stališč na obeh straneh Atlantika, ki bi preživela tudi morebitni ponovni test najvišjih sodnih instanc EU. Možne rešitve vključujejo oblikovanje pravnega nadzora nad uporabo, vpogledom, izmenjavo in obdelavo osebnih podatkov med ZDA in EU preko neodvisnih organov, ki bi lahko presodili, ali je takšno zbiranje podatkov zakonito in sorazmerno.
Bo to dovolj? Težko je reči. Sodišče EU je bilo jasno v sodbi, da državljani EU potrebujejo boljši pravni nadzor, ki naj prepreči, da bi ameriške oblasti morda »napačno« ravnale z njihovimi podatki. Najnovejši predlogi – gre za neformalne informacije iz različnih diplomatskih virov v Bruslju – nakazujejo takšno rešitev. Vendar to ni enak sistem, do katerega imajo državljani članic EU dostop v svojih domačih državah. Ključno bo ustvarjanje enakovrednega (ne pa nujno tudi istovrstnega) niza zaščite zasebnosti za državljane EU. gg

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.