

POGODBA O OBDELAVI OSEBNIH PODATKOV

ODDELEK I

Določilo 1

Namen in področje uporabe

- (a) Namen teh standardnih pogodbenih določil (v nadaljnjem besedilu: določila) je zagotoviti skladnost s členom 28(3) in (4) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
- (b) Upravitelji in obdelovalci na seznamu iz Priloge I soglašajo s temi določili, da se zagotovi skladnost s členom 28(3) in (4) Uredbe (EU) 2016/679.
- (c) Ta določila se uporabljajo za obdelavo osebnih podatkov, kot je določeno v Prilogi II.
- (d) Priloge I do IV so sestavni del določil.
- (e) Ta določila ne posegajo v obveznosti, ki veljajo za upravitelja na podlagi Uredbe (EU) 2016/679.
- (f) Ta določila sama po sebi ne zagotavljajo skladnosti z obveznostmi v zvezi z mednarodnimi prenosi v skladu s poglavjem V Uredbe (EU) 2016/679.

Določilo 2

Nespremenljivost določil

- (a) Pogodbenice se zavezujejo, da ne bodo spreminjale določil, razen dodajanja informacij v priloge ali posodabljanja informacij v njih.
- (b) To pogodbenicam ne preprečuje, da standardna pogodbeni določila iz teh določil vključijo v širšo pogodbo ali dodajo druga določila ali dodatne zaščitne ukrepe, če neposredno ali posredno ne nasprotujejo določilom ali posegajo v temeljne pravice ali svoboščine posameznikov, na katere se nanašajo osebni podatki.

Določilo 3

Razlaga

- (a) Kadar se v teh določilih uporabljajo izrazi, opredeljeni v Uredbi (EU) 2016/679, imajo ti izrazi isti pomen kot v navedeni uredbi.
- (b) Ta določila se berejo in razlagajo v skladu z določbami Uredbe (EU) 2016/679.
- (c) Ta določila se ne razlagajo na način, ki bi bil v nasprotju s pravicami in obveznostmi iz Uredbe (EU) 2016/679, ali na način, ki posega v temeljne pravice ali svoboščine posameznikov, na katere se nanašajo osebni podatki.

Določilo 4

Hierarhija

V primeru neskladja med temi določili in določbami povezanih dogovorov med pogodbenicami, ki obstajajo v času sprejetja dogovora o teh določilih ali so sklenjeni po tem, prevladajo ta določila.

Določilo 5

Določilo o pridružitvah

- (a) Vsak subjekt, ki ni pogodbenica teh določil, se lahko s soglasjem vseh pogodbenic k tem določilom pridruži kadar koli kot upravitelj ali obdelovalec, in sicer tako, da izpolni priloge in podpiše Prilogo I.
- (b) Ko so priloge iz točke (a) izpolnjene in podpisane, se pridružen subjekt obravnava kot pogodbenica teh določil ter ima pravice in obveznosti upravitelja ali obdelovalca v skladu z njegovim imenovanjem v Prilogi I.
- (c) Pridružen subjekt nima nobenih pravic ali obveznosti na podlagi teh določil iz obdobja, preden je postal pogodbenica.

ODDELEK II

OBVEZNOSTI POGODBENIC

Določilo 6

Opis obdelave

Podrobnosti postopkov obdelave, zlasti vrste osebnih podatkov in nameni, za katere se osebni podatki obdelujejo v imenu upravljavca, so določene v Prilogi II.

Določilo 7

Obveznosti pogodbenic

7.1 Navodila

- (a) Obdelovalec obdeluje osebne podatke samo po dokumentiranih navodilih upravljavca, razen če to od njega zahteva pravo Unije ali pravo 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. Upravljavec lahko med celotnim trajanjem obdelave osebnih podatkov da tudi nadaljnja navodila. Ta navodila se vedno dokumentirajo.
- (b) Obdelovalec nemudoma obvesti upravljavca, če po mnenju obdelovalca navodila upravljavca kršijo Uredbo (EU) 2016/679 ali veljavne določbe Unije ali države članice o varstvu podatkov.

7.2 Omejitev namena

Obdelovalec obdeluje osebne podatke samo za posebne namene obdelave, kot je določeno v Prilogi II, razen če od upravljavca prejme nadaljnja navodila.

7.3 Trajanje obdelave osebnih podatkov

Obdelovalec lahko osebne podatke obdeluje le toliko časa, kot je določeno v Prilogi II.

7.4 Varnost obdelave

- (a) Obdelovalec izvaja vsaj tehnične in organizacijske ukrepe iz Priloge III, da zagotovi varnost osebnih podatkov. To vključuje zaščito podatkov pred kršitvijo njihove varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do podatkov (v nadaljnjem besedilu: kršitev varnosti osebnih podatkov). Pri določanju ustrezne ravni varnosti pogodbenice ustrezno upoštevajo najnovejši tehnološki razvoj, stroške izvajanja ter naravo, obseg, okoliščine in namene obdelave ter s tem povezana tveganja za posameznike, na katere se nanašajo osebni podatki.
- (b) Obdelovalec članom svojega osebja odobri dostop do osebnih podatkov, ki se obdelujejo, zgolj v obsegu, ki je nujno potreben za izvajanje, upravljanje in spremljanje pogodbe. Obdelovalec zagotovi, da so osebe, ki so pooblaščen za obdelavo prejetih osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon.

7.5 Občutljivi podatki

Če obdelava vključuje osebne podatke, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, genetske podatke ali biometrične podatke za namene edinstvene identifikacije posameznika, podatke v zvezi z zdravjem ali spolnim življenjem ali spolno usmerjenostjo posameznika ali podatke v zvezi s kazenskimi obsodbami in kaznivimi dejanji („občutljivi podatki“), obdelovalec uporabi posebne omejitve in/ali dodatne zaščitne ukrepe.

7.6 Dokumentacija in skladnost

- (a) Pogodbenice so sposobne dokazati skladnost s temi določili.
- (b) Obdelovalec nemudoma in ustrezno obravnava poizvedbe upravljavca v zvezi z obdelavo podatkov v skladu s temi določili.
- (c) Obdelovalec da upravljavcu na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti, ki so določene v teh določilih in izhajajo neposredno iz Uredbe (EU) 2016/679. Obdelovalec na zahtevo upravljavca prav tako dovoli revizije dejavnosti obdelave, ki jih zajemajo ta določila, in k njim prispeva v razumnih časovnih presledkih ali v primeru znakov neskladnosti. Upravljavec lahko pri odločanju o pregledu ali reviziji upošteva ustrezne certifikate obdelovalca.
- (d) Upravljavec se lahko odloči, da bo revizijo izvedel sam ali pooblastil neodvisnega revizorja. Revizije lahko vključujejo tudi inšpekcijske preglede v prostorih ali fizičnih objektih obdelovalca in se po potrebi izvedejo v razumnem roku od obvestila o njih.
- (e) Pogodbenice pristojnemu nadzornemu organu oziroma organom na zahtevo omogočijo dostop do informacij iz tega določila, vključno z rezultati revizij.

7.7 Uporaba podobdelovalcev

- (a) Obdelovalec ima splošno dovoljenje upravljavca za najem podobdelovalcev z dogovorjenega seznama. Obdelovalec posebej pisno obvesti upravljavca o vseh nameranih spremembah tega seznama z dodajanjem ali zamenjavo podobdelovalcev vsaj 15 dni vnaprej, s čimer upravljavcu zagotovi dovolj časa, da lahko ugovarja takšnim spremembam, preden je zadevni podobdelovalec najet. Obdelovalec zagotovi upravljavcu informacije, ki jih slednji potrebuje za uveljavljanje pravice do ugovora.
- (b) Kadar obdelovalec najame podobdelovalca za izvajanje posebnih dejavnosti obdelave (v imenu upravljavca), to stori s pogodbo, ki podobdelovalcu nalaga vsebinsko enake obveznosti glede varstva podatkov, kot jih ima obdelovalec podatkov v skladu s temi določili. Obdelovalec zagotovi, da podobdelovalec izpolnjuje obveznosti, ki veljajo za obdelovalca v skladu s temi določili ter Uredbo (EU) 2016/679.
- (c) Obdelovalec na zahtevo upravljavca slednjemu zagotovi kopijo take pogodbe s podobdelovalcem in vseh njenih naknadnih sprememb. Kolikor je to potrebno za varovanje poslovnih skrivnosti ali drugih zaupnih informacij, vključno z osebnimi podatki, lahko obdelovalec pred posredovanjem kopije zakrije občutljive in zaupne dele pogodbe.
- (d) Obdelovalec ostane v celoti odgovoren upravljavcu za izpolnjevanje obveznosti podobdelovalca v skladu z njegovo pogodbo z obdelovalcem. Obdelovalec obvesti upravljavca, če podobdelovalec ne izpolnjuje več svojih pogodbenih obveznosti.
- (e) Obdelovalec se s podobdelovalcem dogovori o klavzuli v korist tretjega, v skladu s katero ima upravljavec, če obdelovalec dejansko izgine, pravno preneha obstajati ali postane insolventen, pravico, da odpove pogodbo podobdelovalca in naroči podobdelovalcu, naj izbriše ali vrne osebne podatke.

7.8 Mednarodni prenosi podatkov

- (a) Obdelovalec lahko podatke tretji državi ali mednarodni organizaciji prenese le na podlagi dokumentiranih navodil upravljavca ali zaradi izpolnjevanja posebne zahteve v skladu s pravom Unije ali pravom države članice, ki velja za obdelovalca, in sicer v skladu s poglavjem V Uredbe (EU) 2016/679.
- (b) Upravljavec soglaša, da kadar obdelovalec v skladu z določilom 7.7 za izvajanje posebnih dejavnosti obdelave (v imenu upravljavca) najame podobdelovalca in te dejavnosti obdelave vključujejo prenos osebnih podatkov v smislu poglavja V Uredbe (EU) 2016/679, lahko obdelovalec in podobdelovalec zagotovita skladnost s poglavjem V Uredbe (EU) 2016/679 z uporabo standardnih pogodbenih določil, ki jih je sprejela Komisija v skladu s členom 46(2) Uredbe (EU) 2016/679, če so izpolnjeni pogoji za uporabo navedenih standardnih pogodbenih določil.

Pomoč upravljavcu

- (a) Obdelovalec nemudoma obvesti upravljavca o vsaki zahtevi, ki jo je prejel od posameznika, na katerega se nanašajo osebni podatki. Na to zahtevo se ne odzove sam, razen če ga za to pooblasti upravljavec.
- (b) Obdelovalec pomaga upravljavcu pri izpolnjevanju njegovih obveznosti odzivanja na zahteve posameznikov, na katere se nanašajo osebni podatki, za uveljavljanje njihovih pravic, pri čemer upošteva naravo obdelave. Obdelovalec pri izpolnjevanju svojih obveznosti v skladu s točkama (a) in (b) ravna v skladu z navodili upravljavca.
- (c) Poleg obveznosti, da pomaga upravljavcu v skladu z določilom 8(b), obdelovalec pomaga upravljavcu pri zagotavljanju izpolnjevanja naslednjih obveznosti, pri čemer upošteva naravo obdelave podatkov in informacije, ki so mu na voljo:
 - (1) obveznost izvedbe ocene učinka predvidenih postopkov obdelave na varstvo osebnih podatkov (v nadaljnjem besedilu: ocena učinka v zvezi z varstvom podatkov), kadar je verjetno, da bo vrsta obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov;
 - (2) obveznost posvetovanja s pristojnim nadzornim organom oziroma organi pred obdelavo, kadar je iz ocene učinka v zvezi z varstvom podatkov razvidno, da bi obdelava povzročila veliko tveganje, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja;
 - (3) obveznost, da zagotovi točnost in ažurnost osebnih podatkov, in sicer s takojšnjo obvestitvijo upravljavca, če obdelovalec ugotovi, da so osebni podatki, ki jih obdeluje, netočni ali zastareli;
 - (4) obveznosti iz člena 32 Uredbe (EU) 2016/679.
- (d) Pogodbenice v Prilogi III določijo ustrezne tehnične in organizacijske ukrepe, s katerimi obdelovalec upravljavcu pomaga pri uporabi tega določila, ter področje in obseg potrebne pomoči.

Določilo 9

Obvestilo o kršitvi varnosti osebnih podatkov

V primeru kršitve varnosti osebnih podatkov obdelovalec sodeluje z upravljavcem in mu pomaga pri izpolnjevanju njegovih obveznosti iz členov 33 in 34 Uredbe (EU) 2016/679, kadar je ustrezno, pri čemer upošteva naravo obdelave in informacije, ki so mu na voljo.

9.1 Kršitev varstva podatkov v zvezi s podatki, ki jih obdeluje upravljavec

V primeru kršitve varnosti osebnih podatkov v zvezi s podatki, ki jih obdeluje upravljavec, obdelovalec upravljavcu pomaga pri:

- (a) obveščanju pristojnega nadzornega organa oziroma organov o kršitvi varnosti osebnih podatkov brez nepotrebnega odlašanja po seznanitvi upravljavca s kršitvijo, kadar je to ustrezno (razen če ni verjetno, da bi kršitev varnosti osebnih podatkov povzročila tveganje za pravice in svoboščine posameznikov);
- (b) pridobivanju naslednjih informacij, ki se v skladu s členom 33(3) Uredbe (EU) 2016/679 navedejo v uradnem obvestilu upravljavca in morajo vključevati vsaj:
 - (1) vrsto osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter kategorije in približno število zadevnih evidenc osebnih podatkov;
 - (2) verjetne posledice kršitve varnosti osebnih podatkov;
 - (3) ukrepe, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varnosti osebnih podatkov, vključno z ukrepi za ublažitev morebitnih škodljivih učinkov kršitve, če je ustrezno.

Kadar in kolikor vseh teh informacij ni mogoče zagotoviti hkrati, začetno obvestilo vsebuje informacije, ki so takrat na voljo, nadaljnje informacije pa se takoj, ko so na voljo, predložijo brez nepotrebnega odlašanja;

- (c) izpolnjevanju obveznosti v skladu s členom 34 Uredbe (EU) 2016/679, da se posameznik, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja obvesti o kršitvi varnosti osebnih podatkov, kadar je verjetno, da bo kršitev varnosti osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov.

9.2 Kršitev varstva podatkov v zvezi s podatki, ki jih obdeluje obdelovalec

V primeru kršitve varnosti osebnih podatkov v zvezi s podatki, ki jih obdeluje obdelovalec, obdelovalec o tem nemudoma obvesti upravljavca, potem ko je izvedel za kršitev. Tako obvestilo zajema vsaj:

- (a) opis narave kršitve (po možnosti vključno s kategorijami in približnim številom zadevnih posameznikov, na katere se nanašajo osebni podatki, ter kategorijami in približnim številom zadevnih evidenc osebnih podatkov);
- (b) podrobnosti o kontaktni točki, kjer je mogoče dobiti več informacij o kršitvi varnosti osebnih podatkov;
- (c) verjetne posledice kršitve in ukrepe, ki so bili sprejeti ali katerih sprejetje je bilo predlagano za obravnavanje kršitve, vključno z ukrepi za ublažitev njenih morebitnih škodljivih učinkov.

Kadar in kolikor vseh teh informacij ni mogoče zagotoviti hkrati, začetno obvestilo vsebuje informacije, ki so takrat na voljo, nadaljnje informacije pa se takoj, ko so na voljo, predložijo brez nepotrebnega odlašanja.

Pogodbenice v Prilogi III določijo vse druge elemente, ki jih mora obdelovalec zagotoviti, ko upravljavcu pomaga pri izpolnjevanju obveznosti upravljavca iz členov 33 in 34 Uredbe (EU) 2016/679.

ODDELEK III

KONČNE DOLOČBE

Določilo 10

Neskladnost z določili in odpoved pogodbe

- (a) Brez poseganja v katere koli določbe Uredbe (EU) 2016/679 lahko upravljavec v primeru, da obdelovalec krši svoje obveznosti iz teh določil, naroči obdelovalcu, naj začasno prekine obdelavo osebnih podatkov, dokler slednji ne zagotovi skladnosti s temi določili, sicer pogodbo odpove. Obdelovalec takoj obvesti upravljavca, če iz kakršnega koli razloga ne more zagotoviti skladnosti s temi določili.
- (b) Upravljavec ima pravico, da odpove pogodbo, kolikor zadeva obdelavo osebnih podatkov v skladu s temi določili, če:
 - (1) je upravljavec obdelavo osebnih podatkov, ki jo izvaja obdelovalec, začasno prekinil v skladu s točko (a) in če skladnost s temi določili ni ponovno vzpostavljena v razumnem roku, v vsakem primeru pa v enem mesecu po začasni prekinitvi;
 - (2) obdelovalec znatno ali vztrajno krši ta določila ali svoje obveznosti na podlagi Uredbe (EU) 2016/679;
 - (3) obdelovalec ne ravna v skladu z zavezujočo odločbo pristojnega sodišča ali pristojnega nadzornega organa oziroma organov glede njegovih obveznosti v skladu s temi določili oziroma Uredbo (EU) 2016/679.
- (c) Obdelovalec ima pravico, da odpove pogodbo, kolikor zadeva obdelavo osebnih podatkov v skladu s temi določili, če upravljavec po tem, ko ga je obdelovalec obvestil, da njegova navodila kršijo veljavne pravne zahteve v skladu z določilom 7.1(b), vztraja pri upoštevanju navodil.
- (d) Obdelovalec po odpovedi pogodbe v skladu z odločitvijo upravljavca izbriše vse osebne podatke, ki jih je obdelal v imenu upravljavca, in upravljavcu potrdi, da je to storil, ali vse osebne podatke vrne upravljavcu in izbriše obstoječe kopije, razen če pravo Unije ali pravo države članice zahteva hrambo osebnih podatkov. Obdelovalec zagotavlja skladnost s temi določili, dokler se podatki ne izbrišejo ali vrnejo.

PRILOGA I

Seznam pogodbenic

Upravljavci: *[Identiteta in kontaktni podatki upravljavcev ter po potrebi pooblaščne osebe za varstvo podatkov pri upravljavcu]*

Slovenski inštitut za revizijo

Dunajska 106

1000 Ljubljana

Dr. Samo Javornik, direktor

Obdelovalec:

GO-LIX d.o.o.

Cesta Goriške fronte 46

5290 Šempeter pri Gorici

Boštjan Špehonja, direktor

PRILOGA II

Opis obdelave

Kategorije posameznikov, na katere se nanašajo osebni podatki in katerih osebni podatki se obdelujejo:

- zaposleni pri upravljavcu in drugi posamezniki, ki delujejo v okviru upravljavca.

Vrste osebnih podatkov, ki se obdelujejo:

- osnovni podatki o uporabniku (ime, priimek, e-naslov),
- generirani podatki na platformi (izidi testiranja, opravljeni tečaji, odzivi pri testih).

Obdelava posebnih vrst (občutljivih) osebnih podatkov se ne izvaja.

Narava obdelave

- Posredovanje, sledenje za namen izobraževanja, prikaz rezultatov upravljavcu.

Nameni, za katere se osebni podatki obdelujejo v imenu upravljavca

- Registracija in prijava na platformo PhishStrike, izvedba testiranja, udeležba in rezultati izobraževanja.

Trajanje obdelave

- Do izteka vsakokratne pogodbe o storitvah oz. naročnine.

PRILOGA III

Tehnični in organizacijski ukrepi, vključno s tehničnimi in organizacijskimi ukrepi za zagotovitev varnosti podatkov

- ukrepi za psevdonimizacijo in šifriranje osebnih podatkov;
- ukrepi za zagotovitev stalne zaupnosti, celovitosti, dostopnosti in odpornosti sistemov in storitev za obdelavo;
- ukrepi za zagotovitev zmožnosti pravočasne povrnitve razpoložljivosti in dostopa do osebnih podatkov v primeru fizičnega ali tehničnega incidenta;
- postopki rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotovitev varnosti obdelave;
- ukrepi za identifikacijo uporabnika in izdajo dovoljenja uporabniku;
- ukrepi za varstvo podatkov med prenosom;
- ukrepi za varstvo podatkov med hrambo;
- ukrepi za zagotavljanje fizične varnosti lokacij, na katerih se obdelujejo osebni podatki;
- ukrepi za zagotavljanje beleženja dogodkov;
- ukrepi za zagotavljanje konfiguracije sistema, vključno s privzeto konfiguracijo;
- ukrepi za notranje upravljanje in vodenje IT in varnosti IT;
- ukrepi za zagotavljanje najmanjšega obsega podatkov;
- ukrepi za zagotavljanje kakovosti podatkov;
- ukrepi za zagotavljanje omejene hrambe podatkov;
- ukrepi za zagotavljanje odgovornosti;
- ukrepi za omogočanje prenosljivosti podatkov in zagotavljanje izbrisa.

Vsak podobdelovalec je dolžan izpolnjevati vsaj isti nivo varnosti obdelave, kot je ta določena med upravljavcem in obdelovalcem.

PRILOGA IV

Seznam podobdelovalcev

Upravljavec je odobril uporabo naslednjih podobdelovalcev:

- Webtasy, spletne storitve, d.o.o., Pod hribom 55, 1000 Ljubljana, Matična številka: 1883763000 [poštni strežnik, preko katerega se pošiljajo elektronska sporočila]
- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany [IaaS]
- POSITIVA REŠITVE, informacijske tehnologije, d.o.o., Tržaška cesta 286D, 1000 Ljubljana Matična številka: 6486207000 [Razvijalci aplikacije]
- <https://www.typeform.com/dpa> [Ponudnik spletnih kvizov, ki obdeluje le psevdonimizirane podatke]