Iskraemeco varnostna politika za oblačne storitve

www.iskraemeco.com

Vloge in odgovornosti v oblačnih storitvah

Ponudnik oblačnih storitev (ang. Cloud Service Provider): Družba Iskraemeco, d.d. (v nadaljevanju Iskraemeco) je odgovorna za zagotavljanje oblačnih storitve svojim strankam in je v tem primeru obdelovalec podatkov strank oblačnih storitev in njenih uporabnikov. Iskraemeco pri zagotavljanju oblačnih storitev ravna v skladu s standardi in zakonodajo za varovanje osebnih in drugih podatkov ter sprejetimi organizacijskimi predpisi.

Stranka oblačnih storitev (ang. Cloud Service Customer): Stranka oblačnih storitev (v nadaljevanju stranka), ki vstopa v pogodbeno razmerje z Iskraemecom je dolžna spoštovati določila te politike, pogodb in splošnih pogojev poslovanja. Stranka je kot upravljavec podatkov svojih uporabnikov oblačnih storitev Iskraemeca odgovorna za:

- ravnanje v skladu s tehničnimi navodili za uporabo oblačnih storitev in to varnostno politiko,
- upravljanje z osebnimi in drugimi podatki njenih uporabnikov in spoštovanje veljavne zakonodaje,
- določanje zahtev glede obdelave osebnih in drugih podatkov in
- spreminjanje podatkov, za zagotavljanje ažurnosti in točnosti.

Uporabnik oblačnih storitev (ang. Cloud Service User): Za uporabnika oblačnih storitev se smatra zaposlenega pri stranki (npr. administratorja oblačnega okolja stranke), zaposlenega pri Iskraemecu, če je s stranko sklenjena pogodba za celovito upravljanje oblačne storitve ali končnega odjemalca stranke, katerega podatki se obdelujejo v okviru oblačne storitve.

Obdelovalec podatkov oblačnih storitev (ang. Data Processor): Iskraemeco je obdelovalec podatkov oblačnih storitev, med katere štejejo podatki o aktivnosti strank in posredovani osebni in drugi podatki o njenih uporabnikih. Kot obdelovalec podatkov, je Iskraemeco odgovoren za ravnanje v skladu z veljavno zakonodajo in pogodbenimi zahtevami, ki jih določi stranka, kar lahko zajema:

- Zagotavljanje varnosti obdelave osebnih podatkov;
- vodenje evidence dejavnosti obdelav,
- sodelovanje z nadzornimi organi,
- obveščanje upravljavca v primeru kršitev ali varnostnih incidentov,
- pridobivanje predhodnega pisnega dovoljenja upravljavca, za angažiranje pod-obdelovalcev in
- spoštuje veljavno zakonodajo na področju varovanja osebnih in drugih podatkov.

Ponudniki storitev (angl. Third Party Suppliers): Ponudniki storitev so dobavitelji, ki Iskraemecu zagotavljajo zmogljivosti za izvajanje storitev ob tem pa postavljajo lastne pogoje. Ponudniki storitev morajo pri zagotavljanju storitev slediti varnostnim zahtevam določenim v pogodbah in veljavni zakonodaji na področju varstva osebnih in drugih podatkov. Ponudnik storitev ima lahko dostop do osebnih in drugih podatkov za namen in v obsegu, v katerem jih potrebuje za izvajanje storitev.

Odgovorni za varnost, pravo in skladnost poslovanja (ang. Security, Legal and Compliance Team): zagotavljajo kontaktno točko za odgovore na vprašanja glede varstva osebnih in drugih podatkov, varstva intelektualne lastnine, prijav in razrešitev varnostnih incidentov vezanih na oblačne storitve, kar lahko zajema:

- obveščanje o razkritju osebnih in drugih podatkov,
- skladnost z zakonodajo in standardi in
- ocenjevanje varnostnih tveganj.

V Iskraemecu je za zagotavljanje informacijske varnosti odgovoren sektor informacijske varnosti pod okriljem Pooblaščenca za informacijsko varnost. Sektor skrbi za upravljanje varnostnih postopkov in varnostnih politik ter nadzor nad izvajanjem varnostnih kontrol standardov in veljavne zakonodaje. V vseh sistemih se izvajajo redni varnostni pregledi, ocene varnostnih tvegan, spremljava in odpravljanje ranljivosti.

Za zagotavljanje visokega nivoja varnosti podatkov morajo stranke slediti usmeritvam varnostnih politik in produktne dokumentacije. V tej politiki so opredeljena določila v zvezi z zagotavljanjem ustreznih varnostnih kontrol in varovanjem podatkov v oblačnih storitvah Iskraemeca. Politika dopolnjuje interne organizacijske predpise, splošne pogoje poslovanja in določila pogodb, ki veljajo za produkte in storitve Iskraemeca.

Skladnost

Ustrezno varovanje informacij in informacijskega sistema je ključnega pomena za poslovanje Iskraemeca. Ob spremembah zakonodaje, spremembah v organiziranosti podjetja in storitvah, pojavu novih groženj, incidentov in spremembah tehnične infrastrukture, ki vplivajo na varovanje informacij in informacijskega sistema, se bo sistem upravljanja varovanja informacij nenehno prilagajal z uvajanjem novih in dopolnjevanjem, že obstoječih postopkov ter varnostnih ukrepov.

Iskraemeco je podvržen rednim letnim revizijskim pregledom, vezanim na izpolnjevanje skladnosti vzpostavljenega Sistema upravljanja informacijske varnosti (SUIV), zato je dolžno upoštevati vse zahteve standardov ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 ter veljavne zakonodaje.

Vsako neupoštevanje pravil internih organizacijskih predpisov Iskraemeca, varnostnih politik ter postopkov in navodil se šteje za kršitev in se kot tako tudi ustrezno sankcionira.

Vse interne varnostne organizacijske predpise, varnostne politike in navodila Iskraemeco hrani še vsaj pet let od ukinitve ali nadomestitve z novim dokumentom.

Skladnost z zakonskimi zahtevami

Delovanje Iskraemeca, mora biti v skladu z veljavnimi zakonskimi in podzakonskimi akti, z ratificiranimi mednarodnimi pogodbami in s primarno in sekundarno zakonodajo Evropske Unije.

Vodstvo se zavezuje in zagotavlja, da podjetje posluje v skladu z vso veljavno zakonodajo in ostalimi veljavnimi zakonskimi okviri.

Vodstvo je odgovorno, po potrebi skupaj s pravno službo, za spremljanje sprememb zakonodaje in ostalih zakonskih okvirov. V primeru zakonskih sprememb, vezanih na varovanje informacij, Iskraemeco ustrezno uskladi dokumentirani Sistem upravljanja informacijske varnosti (SUIV).

Za skladnost z veljavno zakonodajo je odgovorna pravna služba Iskraemeca.

Komunikacija s stranko

Iskraemeco stranko obvešča o pomembnih informacijah o delovanju oblačnih storitev, kar lahko zajema:

- predhodno obveščanje o pomembnih spremembah in vzdrževalnih delih v oblačnih storitvah in/ali pri ponudnikih storitev in
- obveščanje o zaznanih varnostnih incidentih, tveganjih in ranljivostih, ki so povezani z okoljem oblačnih storitev in/ali ogrožajo varstvo osebnih in drugih podatkov.

Obdelava osebnih in drugih podatkov

Iskraemeco lahko pridobi osebne in druge podatke od stranke neposredno ali posredno prek uporabnikove uporabe posamezne oblačne storitve. Vrste osebnih in drugih podatkov o uporabnikih, ki jih Iskraemeco obdeluje, vključujejo podatke o seji, povezavi in nastavitvah. To vrsto podatkov hrani v obliki sistemskih zapisov in pri tem zagotovi ustrezno raven varnosti podatkov, kot je navedeno v poglavju varnost hranjenja.

Iskraemeco obdeluje osebne in druge podatke izključno v skladu z namenom, navodili in zahtevami stranke ter legitimnim interesom, kar lahko zajema:

- Analizo uporabe storitev svojih strank in njenih uporabnikov za izboljšanje uporabniške izkušnje, kakovosti in varnosti oblačnih storitev na podlagi uporabe in
- marketinške aktivnosti in oglaševanje.

Hranjenje osebnih in drugih podatkov

Država hranjenja: Osebni in drugi podatki se obdelujejo v državah, kjer se nahajajo podatkovni centri ponudnika oblačnih storitev (Microsoft Azure) in v državah kjer so prostori Iskraemeca. Iskraemeco osebnih podatkov ne iznaša v tretje države. V primerih, ko je potreben iznos v tretje države se to omogoči v skladu z ukrepi za varovanje podatkov, ki veljajo v Iskraemecu ter skladno s pogodbenimi obveznostmi stranke. Seznam podatkovnih centrov Microsoft Azure je dostopen na spletni strani *Global Infrastructure | Microsoft Azure*.

Roki hrambe: Iskraemeco obdeluje osebne in druge podatke za čas veljave pogodbenih razmerij s stranko in do izpolnitve vseh pogodbenih obveznosti. V primeru, ko je hramba osebnih ali drugih podatkov določena s strani veljanje zakonodaje ali drugih veljavnih predpisov, mora Iskraemeco zagotoviti hrambo toliko časa, kot to predvideva zakonski okvir.

Prenehanje hranjenja (izbris/odstranitev podatkov): Po preklicu pogodbe s stranko, Iskraemeco preneha z obdelavo zbranih osebnih in drugih podatkov za namene obdelave, navedene v tej politiki. Po koncu dobe hranjenja, Iskraemeco izvede odstranjevanje osebnih in drugih podatkov v skladu z varnimi praksami za izbris podatkov in skladno s pogodbenimi določili.

Iskraemeco začasne datoteke (npr. sistemske zapise, dokumente), ki vsebujejo osebne in druge podatke izbriše takoj, ko preneha razlog za njihovo hrambo.

Načini varnega hranjenja podatkov

Informacijska varnost: Iskraemeco zagotavlja varnost osebnih in drugih podatkov z varnostnimi ukrepi na področjih tehnične varnosti, fizične varnosti, varnosti komunikacij, operacij in človeških virov. Pri nadzoru sistemov Iskraemeco uporablja preverjene varnostne rešitve in sledi najboljšim varnostnim praksam. Razvoj in izvajanje oblačnih storitev potekata v varnem okolju in v skladu z varnostnimi kontrolami, ki jih predvidevajo standardi ISO/IEC 27001, ISO/IEC 27017 in ISO/IEC 27018, kar lahko zajema:

- Zaščito transakcij aplikacijskih storitev,
- zagotavljanje koncepta šifriranja podatkov v mirovanju (ang. data encryption at rest) in ob prenosu (ang. data encryption in transit),
- nadzorovanje sprememb,
- načela varnega sistemskega inženiringa,
- varnost hrambe in dostopa do programske izvorne kode,

- varnostno kopiranje kritičnih informacijskih virov (npr. podatkovne baze, virtualno okolje),
- redno spremljavo oblačnih storitev in infrastrukture z vidika zagotavljanja varovanja informacij,
- nadzor in upravljanje tehničnih ranljivosti,
- ločevanje okolij in podatkov, različnih strank z logično segmentacijo omrežij in
- zaščito pred zlonamernimi akterji.

Podrobne informacije o vpeljanih varnostnih kontrolah so podane v tehnični dokumentaciji, internih varnostnih predpisih in navodilih, ki pokrivajo področje oblačne infrastrukture.

Ponudnik storitev (Microsoft), ki zagotavlja zmogljivosti podatkovnega centra ima vzpostavljene varnostne ukrepe, dostopne na spletni strani *Azure security documentation | Microsoft Learn*. Ponudnik storitev, ki zagotavlja zmogljivosti podatkovnega centra zagotavlja skladnost z različnimi varnostnimi standardi, dostopnimi na spletni strani *Azure compliance documentation | Microsoft Learn*.

Posredovanje osebnih in drugih podatkov

Iskraemeco lahko posreduje osebne in druge podatke organom pregona ali drugim državnim organom na podlagi zakonskih zahtev in v skladu s postopki določenimi z zakonom. Vse zahteve za posredovanje osebnih in drugih podatkov morajo biti utemeljene ter imeti pravno podlago. Stranka lahko od Iskraemeca zahteva posredovanje podatkov v skladu s pogodbenimi določili in ureditvami te politike.

Iskraemeco lahko posreduje osebne podatke tretjim osebam le ob predhodni privolitvi stranke in ob pogoju, da zabeleži komu so bili podatki deljeni, kateri podatki so bili deljeni in v katerem časovnem obdobju so bili podatki deljeni. Tretje osebe so lahko ponudniki storitev, ki za zagotavljanje storitve potrebujejo določene osebne ali druge podatke. Tretje osebe z osebnimi in drugimi podatki ravnajo v skladu z veljavno zakonodajo in s pogodbo o obdelavi podatkov, ki jo sklenejo z Iskraemecom pred sodelovanjem. Iskraemeco preveri, ali tretje osebe izpolnjujejo zahteve glede obdelave in varovanja osebnih in drugih podatkov.

Pravice stranke (pritožbe)

Iskraemeco stranki omogoči:

- Vpogled ali izpis osebnih in drugih podatkov ki jih obdeluje Iskraemeco,
- popravek podatkov v primeru da podatki ki jih obdeluje Iskraemeco niso pravilni,
- izbris ali omejitev obdelave osebnih in drugih podatkov,
- ugovor obdelavi osebnih in drugih podatkov na podlagi zakonitega interesa,
- uveljavljanje pravice do prenosljivosti osebnih in drugih podatkov, ki so bili posredovani Iskraemecu.

V primeru če stranka meni, da Iskraemeco pri obdelavi osebnih in drugih podatkov krši njene pravice lahko vloži pritožbo. Stranka uveljavlja pravice in vloži pritožbe, tako da jih v pisni obliki posreduje na e-naslov dpo@iskraemeco.com ali poštni naslov Iskraemeco, d.d., Savska Loka 4, 4000 Kranj. Na prejete zahteve se bo Iskraemeco odzval z ukrepi in informacijami skladno z veljavnimi zakonskimi roki in določili pogodb s stranko.

Varnostni incidenti

Zaznane varnostne dogodke in incidente za področje oblačnih storitev Iskraemeco obravnava prednostno. Iskraemeco stranke obvešča o pomembnih varnostnih dogodkih in incidentih, ki vplivajo na njihovo okolje v oblaku ali na njihovo postavitev, in sicer v obdobju, določenem v pogodbi, ali v skladu z regulativnimi zahtevami. Obveščanje strank Iskraemeco izvede v skladu z dokumentom »Iskraemeco Case Management System and Material Returns Management Process«, ki opredeljuje proces upravljanja z primeri (ang. Case management). Iskraemeco poroča o vseh varnostnih dogodkih ki niso del normalnega delovanja storitve in dogodkih ki bi lahko vplivali na delovanje, kvaliteto, varnost ali obseg delovanja storitve.

Iskraemeco strankam omogoča sporočanje zaznanih varnostnih dogodkov in incidentov, ter zahteva, da stranke o njih poročajo takoj, ko je to možno. Varnostne dogodke in incidente stranke poročajo prek uporabniškega portala za stranke oziroma sistema za »Case Management«, v skladu z zgoraj navedenimi navodili.

Kadar pride do kršitve varstva osebnih podatkov ali incidenta, ki vključuje osebne podatke (npr. razkritje osebnih podatkov) Iskraemeco sledi procesu upravljanja z varnostnimi dogodki in incidenti skladno z varnostnimi politikami, o tem obvesti stranko pri kateri je oškodovani uporabnik ter, po potrebi, pristojne organe, skladno z veljavnimi zakonskimi zahtevami.

Na zahtevo stranke, ter skladno s splošnimi pogoji poslovanja in pogodbenimi obveznostmi, mora Iskraemeco zagotoviti dostop do sistemskih zapisov okolja stranke in ostalih dokaznih informacij v oblačnem okolju. Dostop omogoči na varen način, s katerim prepreči kakršnekoli negativne vplive na digitalne sledi.

Kršitev varnosti osebnih podatkov: Iskraemeco kršitev varnosti osebnih podatkov kot je razkritje ali zloraba osebnih podatkov, obravnava kot varnostni incident. Dolžnost stranke je da zaznane kršitve v storitvah posreduje v obravnavo Iskraemecu. Kršitve varnosti osebnih podatkov v oblačnih storitvah, Iskraemeco obravnava skladno postopkom upravljanja incidentov in veljavnimi zakonskimi zahtevami.

Časovna sinhronizacija

Za zagotavljanje časovne usklajenosti, ki je nujna z vidika natančne časovne določitve dogodkov, mora biti med stranko in Iskraemecom zagotovljena sinhronizacija ur. Usklajenost ur je pomembna za natančnost sistemskih zapisov, ki služijo kot dokazno gradivo pri preiskavah. Iskraemeco na svoji strežniški infrastrukturi, zagotavlja sinhronizacijo ure s standardom UTC prek slovenskega centralnega vira na Arnesu. Sinhronizacija ur je avtomatska s protokolom omrežnega časa, tako da so vse ure na strežnikih in delovnih postajah usklajene.

Politika je oblikovana v skladu z napotki standardov ISO 27001, ISO 27017, ISO 27018 in veljavnimi zakonskimi zahtevami. Politika se redno posodablja in je javno dostopna na spletnih straneh družbe Iskraemeco.