Ugovor o obradi podataka u skladu s člankom 28. OUZP-a (UOP)

(Version: 06.05.2024)

Ovaj Ugovor o obradi podataka nadopunjuje i pobliže određuje obveze zaštite podataka iz glavnog ugovora zaključenog između Ugovornih strana. Ovaj Ugovor o obradi podataka primjenjuje se na sve aktivnosti povezane s glavnim ugovorom u kojima zaposlenici društva Siemens Healthineers ili treće strane koje je angažiralo društvo Siemens Healthineers obrađuju osobne podatke Kupca ili njegovih klijenata.

0. Tumačenje

0.1. Ako se u ovom UOP-u upotrebljavaju pojmovi definirane u OUZP-u, ti pojmovi imaju isto značenje kao u OUZP-u.

0.2. Ovaj UOP čita se i tumači s obzirom na odredbe OUZP-a.

0.3. Ovaj UOP ne smije se tumačiti na način koji je u suprotnosti s pravima i obvezama predviđenima OUZP-om ili na način koji dovodi u pitanje temeljna prava ili slobode ispitanika.

1. Predmet, priroda, svrha, ograničenje svrhe i trajanje obrade

1.1. Ovaj Ugovor o obradi podataka nadopunjuje glavni ugovor zaključen između Ugovornih strana. It applies to the processing of personal data by Siemens Healthineers (the "Processor") on behalf of the Customer (the "Controller") under the main contract and sets out the data protection obligations of the Parties. Poseban opis predmeta, prirode, svrhe i trajanja obrade osobnih podataka koju izvodi društvo Siemens Healthineers za Kupca sadržan je u postojećim i budućim glavnim ugovorima.

1.2. Priroda i svrha obrade: društvo Siemens Healthineers obrađuje osobne podatke u opsegu potrebnom za pružanje usluga navedenih i prihvaćenih u glavnom ugovoru. Društvo Siemens Healthineers ne smije obrađivati osobne podatke u druge svrhe.

1.3. Društvo Siemens Healthineers i Kupac pojedinačno su odgovorni za vlastitu usklađenost s primjenjivim zakonom o zaštiti podataka. Kupac je sâm odgovoran za načine na koje je Kupac stekao osobne podatke i Kupac će društvu Siemens Healthineers otkriti samo one osobne podatke za koje je dano zakonsko odobrenje i za koje Kupac ima zakonsko pravo na obradu.

1.4. Trajanje obrade odgovara razdoblju trajanja glavnog ugovora.

2. Vrsta osobnih podataka i kategorije ispitanika

Ovisno o odredbama glavnog ugovora kategorije ispitanika čiji se osobni podaci obrađuju posebice su zaposlenici, pacijenti, osobe za kontakt Kupca i ugovorni partneri Kupca. Vrste osobnih podataka uključenih u obradu posebice su kontaktni podaci, identifikatori, podataka o lokaciji, financijski podaci i osjetljivi podaci poput zdravstvenih informacija, genetičkih podataka i biometrijskih podataka.

3. Upute

3.1. Društvo Siemens Healthineers obrađuje osobne podatke isključivo na temelju dokumentiranih uputa Kupca. Ovaj Ugovor o obradi podataka i glavni ugovor predstavljaju potpune i konačne dokumentirane upute Kupca društvu Siemens Healthineers za obradu osobnih podataka.

3.2. Sve dodatne ili alternativne upute Kupac mora dati u pisanom obliku te će one biti obvezujuće samo nakon pisane potvrde društva Siemens Healthineers o primitku. Društvo Siemens Healthineers obavještava Kupca ako se, prema mišljenju društva Siemens Healthineers, uputama koje je dao Kupac krši OUZP ili odredbe o zaštiti podataka koje se primjenjuju na društvo Siemens Healthineers kao izvršitelja obrade. Društvo Siemens Healthineers nema nikakvu obvezu provoditi sveobuhvatnu zakonsku reviziju ni pratiti upute koje su zabranjene zakonom.

3.3. Kupac snosi sve dodatne troškove koji su nastali društvu Siemens Healthineers kao rezultat provedbe dodatne ili alternativne upute, osim ako je uputa potrebna za ostvarivanje usklađenosti sa zakonskim zahtjevima primjenjivima na društvo Siemens Healthineers.

4. Povjerljivost

Društvo Siemens Healthineers omogućit će pristup osobnim podacima koji se obrađuju članovima svojeg osoblja samo u mjeri u kojoj je izričito neophodno za provedbu i praćenje glavnog ugovora te upravljanje njime. Društvo Siemens Healthineers osigurava da su se osobe ovlaštene za obradu primljenih osobnih podataka obvezale na poštovanje stalne povjerljivosti ili da podliježu odgovarajućim zakonskim obvezama o povjerljivosti.

5. Sigurnost obrade

5.1. Društvo Siemens Healthineers poduzima sve potrebne mjere u skladu s člankom 32. OUZP-a.

5.2. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and in particular the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed, Siemens Healthineers shall implement technical and organizational measures as set out in Attachment TOM.

5.3. Kupac i Siemens Healthineers obvezuju se na to da će se provedbom tehničkih i organizacijskih mjera opisanih u Dodatku TOM osigurati prikladna razina sigurnosti u skladu s OUZP-om i dovoljne zaštitne mjere za zaštitu podataka ispitanika.

5.4. Tehničke i organizacijske mjere opisane u Dodatku TOM podložne su tehničkom napretku i daljnjem razvoju te ih društvo Siemens Healthineers može prilagoditi ako je to moguće pod uvjetom da ta prilagodba ne dovede do niže razine zaštite od one koja je navedena u Dodatku TOM.

6. Podobrađivači

6.1. Društvo Siemens Healthineers neće podugovarati bilo koju od svojih aktivnosti obrade koje se izvode bez prethodnog odobrenja Kupca. Tamo gdje društvo Siemens Healthineers podugovara svoje aktivnosti obrade uz odobrenje Kupca, podobrađivači smiju obrađivati osobne podatke samo u svrhu provođenja aktivnosti za koje su ti osobni podaci dostavljeni društvu Siemens Healthineers te im je zabranjena obrada osobnih podataka u druge svrhe.

Svaki podobrađivač bit će angažiran putem ugovora koji podobrađivaču nameće, u biti, jednake obveze zaštite podataka kao one koje su nametnute društvu Siemens Healthineers u skladu s ovim UOP-om, posebice takav ugovor mora osigurati dostatne zaštitne mjere za provedbu odgovarajućih tehničkih i organizacijskih mjera na takav način da će obrada zadovoljiti zahtjeve OUZP-a, osigurati zaštitu prava dotičnih ispitanika, voditi evidenciju prijenosa podataka i dokumentirati odgovarajuće zaštitne mjere. Na zahtjev Kupca društvo Siemens Healthineers Kupcu će dostaviti primjerak takvog ugovora s podobrađivačem i sve naknadne izmjene i dopune. U mjeri potrebnoj za zaštitu poslovnih tajni ili drugih povjerljivih informacija, uključujući osobne podatke, društvo Siemens Healthineers može urediti tekst ugovora prije dijeljenja primjerka.

6.2. Popis podobrađivača dostupan je na adresi https://fleet.siemens-healthineers.com/welcome. Društvo Siemens Healthineers zadržava pravo povremenog ažuriranja te

internetske stranice. Društvo Siemens Healthineers ima opće ovlaštenje Kupca za angažiranje navedenih društava kao podobrađivača.

Kupac je dužan pretplatiti se na tu internetsku stranicu društva Siemens Healthineers kako bi dobivao informacije o podobrađivačima i planiranim promjenama tog popisa u dodavanju ili zamjeni podobrađivača. Društvo Siemens Healthineers odgovorno je za prikupljanje relevantnih informacija od podobrađivača i održavanje ovog popisa ažurnim.

Angažiranje ili zamjena dodatnog podobrađivača smatra se odobrenom ako društvo Siemens Healthineers o tome unaprijed obavijesti Kupca i ako Kupac na to ne uloži prigovor društvu Siemens Healthineers pisanim putem, uključujući prigovor u elektroničkom obliku, unutar 30 dana od davanja te obavijesti.

6.3. Ako Kupac ulaže prigovor, dužan je podrobno obavijestiti društvo Siemens Healthineers o razlozima ulaganja prigovora.

Nakon prigovora društvo Siemens Healthineers može prema vlastitom nahođenju

(i) predložiti drugog podobrađivača umjesto onog koji je odbačen, ili

(ii) poduzeti korake da razriješi zabrinutosti Kupca i tako riješi prigovor Kupca.

6.4. Ako mogućnosti iz članka 6. stavka 3. točki a. i b. nisu razumno dostupne ili prigovor nije na drugi način riješen, društvo Siemens Healthineers može u cijelosti ili djelomično raskinuti glavni ugovor bez prethodne obavijesti, primjerice ako prigovor Kupca znatno otežava ili onemogućuje društvu Siemens Healthineers ispunjavanje ugovornih obveza.

6.5. Svi sporazumi o vremenu odgovora ili dostupnosti bit će raskinuti, a bilo kakvi zahtjevi za naknadom štete umjesto izvršenja, u slučaju kašnjenja ili dogovorenih ugovornih kazni ili sankcija u pogledu društva Siemens Healthineers ne primjenjuju se na podobrađivača od planiranog datuma početka prigovora nadalje. Ako su obveze izvršenja društva Siemens Healthineers djelomično raskinute, naknada za usluge na koju ne utječe djelomični raskid ugovora određuje se u skladu sa standardnim cjenikom društva Siemens Healthineers primjenjivim na takve usluge u društvu Siemens Healthineers.

6.6. U slučajevima kad podobrađivač ne može izvršiti svoje obveze povezane sa zaštitom podataka, društvo Siemens Healthineers i dalje je potpuno odgovorno Kupcu za izvršenje obveza podobrađivača, u skladu s odredbama o odgovornosti iz glavnog ugovora. Društvo Siemens Healthineers nije odgovorno za naknade štete i potraživanja koja su rezultat dodatnih ili alternativnih uputa Kupca prema članku 3. stavku 2. ovog UOP-a.

6.7. U slučaju da je angažiran podobrađivač u trećoj zemlji (izvan EU-a/EGP-a), upotrebljavat će se mehanizmi prijenosa podataka u skladu s člancima OUZP-a 44. i dalje.

6.8. Kupac je suglasan da, kada je podobrađivač angažiran u skladu s ovim člankom 6. za obavljanje specifičnih aktivnosti obrade (uime Kupca) i te aktivnosti obrade uključuju prijenos osobnih podataka u smislu članaka OUZP-a 44. i dalje, usklađenost s člancima OUZP-a 44. i dalje može se osigurati uporabom standardnih klauzula o zaštiti podataka koje je usvojila Komisija u skladu s člankom 46. stavkom 2. OUZP-a, pod uvjetom da su ispunjeni uvjeti za uporabu tih standardnih klauzula o zaštiti podataka ili uporabom drugih odgovarajućih zaštitnih mjera u skladu s člankom 46. OUZP-a.

7. Pomoć

7.1. Uzimajući u obzir prirodu obrade kako je opisano u glavnom ugovoru i ovom Ugovoru o obradi podataka, društvo Siemens Healthineers pomaže Kupcu na zahtjev i o trošku Kupca putem odgovarajućih tehničkih i organizacijskih mjera, koliko je to moguće, da ispuni obvezu Kupca u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika koja su utvrđena u člancima 12. do 23. OUZP-a.

7.2. Društvo Siemens Healthineers bez nepotrebnog odgađanja obavještava Kupca o zahtjevima ispitanika za ostvarivanje njihovih prava prema člancima 12. do 23. OUZP-a, posebice u pogledu prava na pristup osobnim podacima, prava na ispravak, prava na brisanje („pravo na zaborav“), prava na ograničenje obrade, prava na prenosivost podataka, prava na prigovor i prava da ne budu podložni automatskom pojedinačnom odlučivanju.

7.3. Uzimajući u obzir prirodu obrade kao što je opisano u glavnom ugovoru i ovom UOP-u te informacije dostupne u društvu Siemens Healthineers, društvo Siemens Healthineers pomoći će Kupcu na Kupčev trošak u osiguravanju Kupčeve vlastite usklađenosti s obvezama u skladu s

(i) člankom 32. OUZP-a (sigurnost obrade)

(ii) člankom 33. OUZP-a (Izvješćivanje nadzornog tijela o povredi osobnih podataka)

U slučaju povrede osobnih podataka povezane s osobnim podacima koje obrađuje društvo Siemens Healthineers, društvo Siemens Healthineers obavijestit će Kupca bez nepotrebnog odgađanja nakon što društvo Siemens Healthineers sazna za povredu. Takva obavijest mora sadržavati barem:

a. opis prirode povrede (uključujući, gdje je to moguće, kategorije i približan broj predmetnih ispitanika i zapisa podataka)

b. pojedinosti kontaktne točke na kojoj se može dobiti više informacija o povredi osobnih podataka

c. vjerojatne posljedice povrede i mjere koje su poduzete ili predložene za rješavanje povrede, uključujući ublažavanje njezinih mogućih negativnih učinaka.

U slučaju i u mjeri u kojoj nije moguće pružiti sve te informacije istodobno, početna obavijest sadržava informacije koje su tada bile dostupne, a daljnje informacije naknadno će se dostaviti bez nepotrebnog odgađanja kada postanu dostupne.

(iii) članom 34. OUZP-a (Obavješćivanje ispitanika o povredi osobnih podataka)

(iv) člankom 35. OUZP-a (Procjena učinka na zaštitu podataka)

(v) člankom 36. OUZP-a (Prethodno savjetovanje).

7.4. Ako je Kupcu potrebna pomoć, Kupac se može obratiti Uredu službenika za privatnost podataka društva Siemens Healthineers na adresi dataprivacy.func@siemens-healthineers.com.

8. Brisanje

Po izboru Kupca svi se osobni podaci Kupca brišu ili vraćaju nakon završetka pružanja usluga u vezi s obradom. Kupac ovime upućuje društvo Siemens Healthineers da obriše sve osobne podatke Kupca nakon dovršetka pružanja usluga povezanih s obradom te da obriše postojeće primjerke osim ako u skladu s pravom Unije ili pravom države članice postoji obveza pohrane osobnih podataka. Dok se podaci ne izbrišu, društvo Siemens Healthineers nastavit će osiguravati poštovanje ovog UOP-a.

9. 9.Prava na pristup informacijama i reviziju

9.1. U pogledu obrade iz glavnog ugovora društvo Siemens Healthineers na Kupčev pisani zahtjev Kupcu na raspolaganje stavlja sve potrebne informacije kojima dokazuje usklađenost s obvezama iz članka 28. OUZP-a.

9.2. Društvo Siemens Healthineers dopušta i sudjeluje u revizijama Kupca, uključujući inspekcije („revizije“), u pogledu obrade iz glavnog ugovora kojima dokazuje usklađenost s obvezama iz članka 28. OUZP-a. Te revizije može provesti i nezavisni revizor treće strane kojeg je angažirao Kupac pod uvjetom da je taj revizor prihvatljiv društvu Siemens Healthineers i obvezan dužnošću povjerljivosti koja nije manje ograničavajuća od one koja vrijedi za Kupca u skladu s glavnim ugovorom. Kupac će zatražiti reviziju uz razumnu prethodnu obavijest društvu Siemens Healthineers. Prije revizije Ugovorne strane zajednički će se složiti oko opsega, vremena i trajanja revizije. Kupac

društvu Siemens Healthineers nadoknađuje sve usluge koje je društvo Siemens Healthineers izvršilo u vezi s revizijom prema trenutačnim tarifama za usluge društva Siemens Healthineers, koje se Kupcu stavljaju na raspolaganje na njegov zahtjev.

9.3. Kupac bez odlaganja društvu Siemens Healthineers šalje pisano izvješće s povjerljivim sažetkom opsega i rezultata revizije. Neovisno o navedenom društvo Siemens Healthineers ima pravo upotrebljavati izvješće u vlastite svrhe.

Prilog TOM:

Tehničke i organizacijske mjere (TOM) društva Siemens Healthineers

1. Pseudonimizacija i šifriranje osobnih podataka

Društvo Siemens Healthineers odvaja osobne podatke od obrađenih podataka tako da nije moguće povezati obrađene podatke s osobom čiji je identitet utvrđen ili se može utvrditi bez dodatnih informacija koje se pohranjuju odvojeno i na siguran način. Društvo Siemens Healthineers šifrira osobne podatke s pomoću simetričnih ili asimetričnih ključeva.

2. Povjerljivost, integritet, dostupnost i otpornost sustava i Usluga

2.1 Društvo Siemens Healthineers jamči povjerljivost i cjelovitost poduzimanjem sljedećih mjera:

Kontrola pristupa:

Društvo Siemens Healthineers štiti svoje zgrade odgovarajućim sustavima kontrole pristupa temeljenim na sigurnosnoj klasifikaciji zgrada i na dobro definiranom konceptu odobrenja pristupa. Sve su zgrade osigurane mjerama kontrole pristupa uporabom sustava čitača kartica. Ovisno o kategoriji sigurnosti, imovina, zgrade ili pojedina područja osigurana su dodatnim mjerama. To su posebni pristupni profili, biometrija, podmetači za igle, DES hardverski ključevi, brava za odvajanje, videonadzor i sigurnosno osoblje. Prava pristupa za ovlaštene osobe dodjeljuju se pojedinačno prema definiranim kriterijima. To se odnosi i na vanjske osobe.

Kontrola pristupa sustavu:

Pristup sustavima za obradu podataka daje se samo ovlaštenim korisnicima na temelju koncepta odobrenja utemeljenog na ulozi koristeći se sljedećim mjerama: šifriranje podataka, individualizirano dodjeljivanje zaporki (najmanje 8 znakova, redovit automatski istek zaporke), ID iskaznice zaposlenika s PKI šifriranjem, čuvari zaslona zaštićeni zaporkom u slučaju neaktivnosti, sustavi za otkrivanje provale i sustavi za sprječavanje provale, redovito ažurirani filtri protiv virusa i špijunskog softvera na mreži te na pojedinim računalima i mobilnim uređajima.

Kontrola pristupa podacima:

Pristup osobnim podacima odobrava se na temelju koncepta autorizacije temeljenog na ulozi. Postavljen je sustav upravljanja korisnicima koji mapira bazu podataka korisnika s njihovim ovlaštenjima i dostupan je centralno u mreži radi pretraživanja traženjem sustava za obradu podataka. Nadalje, šifriranje podataka sprječava neovlašten pristup osobnim podacima.

Kontrola prijenosa podataka:

Društvo Siemens Healthineers osigurava elektroničke komunikacijske kanale postavljanjem zatvorenih mreža i postupaka šifriranja podataka. Ako se odvija prijenos fizičkih nositelja podataka, provode se provjerljivi prijenosni postupci koji sprječavaju neovlašteni pristup podacima ili logički gubitak. Nositelji podataka odlažu se u skladu s propisima o zaštiti podataka.

2.2 Društvo Siemens Healthineers osigurava stalnu dostupnost i pouzdanost sustava i usluga poduzimanjem sljedećih mjera:

Društvo Siemens Healthineers osigurava dostupnost i otpornost sustava i usluga izoliranjem kritičnih informatičkih i mrežnih komponenti i pružanjem prikladnih sigurnosnih sustava i sustava redundancije, s pomoću sustava redundancije napajanja te redovitim ispitivanjem sustava i usluga. Testni i živi sustavi potpuno su odvojeni.

3. Dostupnost i pristup osobnim podacima u slučaju incidenta

Društvo Siemens Healthineers vraća dostupnost osobnih podataka i pristup njima u slučaju fizičkog ili tehničkog incidenta poduzimanjem sljedećih mjera:

Društvo Siemens Healthineers pohranjuje osobne podatke u sustavima RAID i integrira sustave redundancije u skladu sa sigurnosnom oznakom. Da bi osiguralo napajanje u podatkovnim centrima, društvo Siemens Healthineers upotrebljava sustave za neprekidno napajanje (npr. UPS, akumulatori, generatori).

Baze podataka ili podatkovni centri zrcale se na različitim fizičkim lokacijama.

Dostupan je opsežan pisani plan za slučajeve opasnosti. Procesi i sustavi za izvanredne situacije redovito se pregledavaju.

4. Postupci kontrole kako bi se osigurala sigurnost obrade

Društvo Siemens Healthineers održava postupak kontrole temeljen na pristupu utemeljenom na upravljanju rizikom, uzimajući u obzir osnovne kataloge zaštite informatičke tehnologije Federalnog ureda za sigurnost informacija (BSI) i zahtjeve norme ISO/IEC 27001 za redoviti pregled, procjenu i ocjenu učinkovitosti tehničkih i organizacijskih mjera za osiguranje sigurnosti obrade. Time se osigurava zaštita relevantnih informacija, aplikacija (uključujući metode ispitivanja kvalitete i sigurnosti), operativnih okruženja (npr. praćenjem mreže od štetnih učinaka) i tehničke provedbe koncepta zaštite (npr. pomoću analiza ranjivosti). Sustavnim otkrivanjem i uklanjanjem slabih točaka zaštitne mjere neprestano se preispituju i unaprjeđuju.

5. Kadrovske mjere

Društvo Siemens Healthineers izdaje pisane radne upute i redovito obučava osoblje koje ima pristup osobnim podacima kako bi osiguralo da se osobni podaci obrađuju isključivo u skladu sa zakonom, ovim Ugovorom o obradi podataka i pripadajućim uputama Kupca, uključujući ovdje opisane tehničke i organizacijske mjere.