

Pogodba o obdelavi osebnih podatkov v skladu s členom 28 Splošne uredbe o varstvu podatkov (DPA)

(Različica: 06.05.2024)

Ta pogodba o obdelavi osebnih podatkov dopolnjuje in določa obveznosti glede varstva podatkov iz glavne pogodbe, sklenjene med pogodbenima strankama. Ta pogodba o obdelavi osebnih podatkov velja za vse dejavnosti, ki so povezane z glavno pogodbo in pri katerih zaposleni družbe Siemens Healthineers ali tretje osebe, ki jih najame družba Siemens Healthineers, obdelujejo osebne podatke stranke ali njenih strank.

0. Razlaga pojmov

- 0.1. Kadar se v tej pogodbi o obdelavi osebnih podatkov uporabljajo izrazi, opredeljeni v GDPR, imajo ti izrazi enak pomen kot v GDPR.
- 0.2. Ta pogodba o obdelavi osebnih podatkov se bere in razlaga ob upoštevanju določb GDPR.
- 0.3. Ta pogodba o obdelavi osebnih podatkov se ne sme razlagati na način, ki bi bil v nasprotju s pravicami in obveznostmi, določenimi v GDPR, ali na način, ki bi posegal v temeljne pravice ali svoboščine posameznikov, na katere se nanašajo osebni podatki.

1. Vsebina, narava, namen, omejitev namena in trajanje obdelave

- 1.1. Ta pogodba o obdelavi osebnih podatkov dopolnjuje glavno pogodbo, ki je sklenjena med pogodbenima strankama. Nanaša se na obdelavo osebnih podatkov, ki jo v imenu stranke (»upravljavalec«) v skladu z glavno pogodbo izvaja družba Siemens Healthineers (»obdelovalec«), in določa obveznosti pogodbenih strank glede varstva podatkov. Posebni opis predmeta, narave, namena in trajanja obdelave osebnih podatkov, ki jih družba Siemens Healthineers obdeluje za stranko, je vsebovan v obstoječih in prihodnjih glavnih pogodbah.
- 1.2. Narava in namen obdelave podatkov: družba Siemens Healthineers obdeluje osebne podatke v obsegu, ki je potreben za zagotavljanje storitev, ki so navedene in dogovorjene z glavno pogodbo. Družba Siemens Healthineers ne sme obdelovati osebnih podatkov za druge namene.
- 1.3. Družba Siemens Healthineers in stranka sta vsaka zase odgovorni za spoštovanje veljavne zakonodaje o varstvu podatkov. Stranka je izključno odgovorna za sredstva, s katerimi je pridobila osebne podatke, družba Siemens Healthineers pa lahko razkrije le tiste osebne podatke, za katere je podano zakonsko pooblastilo in za katere ima stranka zakonsko pravico do obdelave.
- 1.4. Trajanje obdelave ustreza trajanju glavne pogodbe.

2. Vrste osebnih podatkov in kategorije posameznikov, na katere se nanašajo osebni podatki

Odvisno od določb glavne pogodbe so kategorije posameznikov, na katere se nanašajo osebni podatki, zlasti zaposleni, pacienti, kontaktne osebe stranke ter pogodbeni partnerji stranke. Vrste osebnih podatkov, vključenih v obdelavo, so zlasti kontaktne informacije, identifikatorji, podatki o lokaciji, finančni podatki in občutljivi podatki, kot so zdravstveni podatki, genetski podatki in biometrični podatki.

3. Navodila

- 3.1. Družba Siemens Healthineers obdeluje osebne podatke le na osnovi dokumentiranih navodil stranke. Ta pogodba o obdelavi osebnih podatkov in glavna pogodba predstavljata popolno in dokončno navodilo stranke družbi Siemens Healthineers za obdelavo osebnih podatkov.
- 3.2. Morebitna dodatna ali nadomestna navodila mora stranka izdati v pisni obliki in so zavezujoča le, če jih družba Siemens Healthineers pisno potrdi. Družba Siemens Healthineers obvesti stranko, če po njenem mnenju navodila stranke kršijo GDPR ali določbe o varstvu podatkov, ki veljajo za družbo Siemens Healthineers kot obdelovalca podatkov. Družbi

Siemens Healthineers ni treba izvesti celovitega pravnega pregleda ali upoštevati navodil, ki so prepovedana z zakonom.

- 3.3. Stranka krije vse dodatne stroške, ki jih ima družba Siemens Healthineers zaradi dodatnega ali nadomestnega navodila, razen če je navodilo potrebno za izpolnitev zakonskih zahtev, ki veljajo za družbo Siemens Healthineers.

4. Zaupnost

Družba Siemens Healthineers odobri dostop do osebnih podatkov v obdelavi članom svojega osebja le v obsegu, ki je nujno potreben za izvajanje, upravljanje in spremljanje glavne pogodbe. Družba Siemens Healthineers zagotavlja, da so se osebe, pooblaščenice za obdelavo prejetih osebnih podatkov, zavezale k stalni zaupnosti ali da zanje velja ustrezna zakonska obveznost zaupnosti.

5. Varnost obdelave

- 5.1. Družba Siemens Healthineers sprejema vse potrebne ukrepe v skladu z 32. členom GDPR.
- 5.2. Ob upoštevanju stanja tehnike, stroškov izvedbe in narave, obsega, konteksta in namena obdelave pa tudi tveganja za spreminjanje verjetnosti in resnosti pravic in svoboščin fizičnih oseb ter zlasti tveganj, ki so prisotna pri obdelavi, še posebej naključno ali nezakonito uničenje, izguba, sprememba, nepooblaščen razkritje ali dostop do osebnih podatkov, ki se prenašajo, shranjujejo ali kako drugače obdelujejo, mora družba Siemens Healthineers izvesti tehnične in organizacijske ukrepe, kot je določeno v prilogi TOM.
- 5.3. Stranka in družba Siemens Healthineers se strinjata, da izvajanje tehničnih in organizacijskih ukrepov, opisanih v prilogi TOM, zagotavlja ustrezno raven varnosti v skladu z GDPR in zagotavlja zadostne zaščitne ukrepe za varstvo pravic posameznika, na katerega se nanašajo osebni podatki.
- 5.4. Tehnični in organizacijski ukrepi, opisani v prilogi TOM, so predmet tehničnega napredka in nadaljnjega razvoja, zato jih lahko družba Siemens Healthineers po potrebi prilagodi, in sicer pod pogojem, da takšna prilagoditev ne povzroči nižje ravni zaščite, kot je določena v prilogi TOM.

6. Podobdelovalci

- 6.1. Družba Siemens Healthineers brez predhodnega dovoljenja stranke ne sme nobene od svojih dejavnosti obdelave podatkov oddati v izvajanje podizvajalcem. Kadar družba Siemens Healthineers s pooblastilom stranke svoje dejavnosti obdelave odda v izvajanje podizvajalcem, lahko podizvajalci obdelujejo osebne podatke le za namene izvajanja dejavnosti, za katere so bili ti osebni podatki posredovani družbi Siemens Healthineers, in ne smejo obdelovati osebnih podatkov za druge namene.

Vsak podobdelovalec mora biti vključen s pogodbo, ki podobdelovalcu nalaga vsebinsko enake obveznosti glede varstva podatkov, kot jih ima družba Siemens Healthineers v skladu s to pogodbo o obdelavi osebnih podatkov, zlasti pa mora takšna pogodba zagotavljati zadostne zaščitne ukrepe za izvajanje ustreznih tehničnih in organizacijskih ukrepov na način, da bo obdelava izpolnjevala zahteve GDPR, zagotavljala varstvo pravic zadevnih posameznikov, na katere se nanašajo osebni podatki, vodila evidence o prenosih podatkov in dokumentirala ustrezne zaščitne ukrepe. Družba Siemens Healthineers mora na zahtevo stranke slednji zagotoviti kopijo takšne pogodbe s podobdelovalcem in vseh naknadnih

sprememb. Če je to potrebno za zaščito poslovnih skrivnosti ali drugih zaupnih informacij, vključno z osebnimi podatki, lahko družba Siemens Healthineers pred posredovanjem kopije redigira besedilo pogodbe.

- 6.2. Seznam podobdelovalcev je voljo na spletni strani: <https://fleet.siemens-healthineers.com/welcome>. Družba Siemens Healthineers si pridržuje pravico do občasne posodobitve tega URL-ja. Družba Siemens Healthineers ima splošno pooblastilo stranke za vključevanje navedenih podjetij kot podobdelovalcev.

Stranka se mora naročiti na to spletno mesto družbe Siemens Healthineers, da bi prejela informacije o podizvajalcih in morebitnih nameranih spremembah tega seznama z dodajanjem ali zamenjavo podizvajalcev. Družba Siemens Healthineers je odgovorna za zbiranje ustreznih informacij od podobdelovalcev in posodabljanje tega seznama.

Šteje se, da je vključitev ali zamenjava dodatnega podobdelovalca odobrena, če družba Siemens Healthineers o tem vnaprej obvesti stranko in če stranka v 30 dneh po tej informaciji družbi Siemens Healthineers pisno, vključno v elektronski obliki, ne ugovarja.

- 6.3. Če stranka ugovarja, mora družbo Siemens Healthineers podrobno obvestiti o razlogih za ugovor.

Na podlagi ugovora lahko družba Siemens Healthineers po lastni presoji

- namesto zavrženega podobdelovalca predlaga drugega podobdelovalca ali
- sprejme ukrepe za odpravo pomislekov stranke, ki odpravljajo njen ugovor.

- 6.4. Če možnosti iz točk a. in b. tretjega odstavka 6. člena razumno niso na voljo ali če ugovor ni bil odpravljen drugače, lahko družba Siemens Healthineers v celoti ali delno odpove glavno pogodbo brez odpovednega roka, npr. če ugovor stranke družbi Siemens Healthineers znatno otežuje ali onemogoča, da bi izpolnila svoje pogodbene obveznosti.

- 6.5. Vsi dogovori o odzivnem času ali razpoložljivosti se začasno prekinajo, morebitni zahtevki v zvezi s tem za odškodnino namesto izpolnitve, za zamudo ali dogovorjeno pogodbeno odškodnino ali pogodbene kazni v zvezi z družbo Siemens Healthineers pa ne veljajo od načrtovanega datuma začetka delovanja podobdelovalca, proti kateremu je bil vložen ugovor, dalje. Če se obveznosti izvedbe družbe Siemens Healthineers delno prekinajo, se nadomestilo za storitve, na katere delna prekinitev ne vpliva, določi v skladu s standardnimi cenami iz cenika družbe Siemens Healthineers, ki veljajo za takšne storitve pri družbi Siemens Healthineers.

- 6.6. Če podobdelovalec ne izpolni svojih obveznosti glede varstva podatkov, je družba Siemens Healthineers – v skladu z določbami o odgovornosti iz glavne pogodbe – še naprej v celoti odgovorna stranki za izpolnitev obveznosti podobdelovalca. Družba Siemens Healthineers ni odgovorna za škodo in zahtevke, ki izhajajo iz dodatnih ali nadomestnih navodil stranke v skladu z drugim odstavkom 3. člena te pogodbe o obdelavi osebnih podatkov.

- 6.7. V primeru vključitve podobdelovalca v tretji državi (zunaj EU/EGP) je treba uporabiti mehanizme za prenos podatkov, ki so skladni s 44. členom in naslednjimi členi GDPR.

- 6.8. Stranka se strinja, da se, če je v skladu s tem 6. členom za izvajanje določenih dejavnosti obdelave (v imenu stranke) vključen podobdelovalec in te dejavnosti obdelave vključujejo prenos osebnih podatkov v smislu 44. člena in naslednjih členov GDPR, skladnost s 44. členom in naslednjimi členi GDPR lahko zagotovi z uporabo standardnih klavzul o varstvu podatkov, ki jih je sprejela Komisija v skladu z drugim odstavkom 46. člena GDPR, če so izpolnjeni pogoji za uporabo teh standardnih klavzul o varstvu podatkov, ali z uporabo drugih ustreznih zaščitnih ukrepov v skladu s 46. členom GDPR.

7. Pomoč

- 7.1. Ob upoštevanju narave obdelave, kot je opisana v glavni pogodbi in tej pogodbi o obdelavi osebnih podatkov, bo družba Siemens Healthineers na zahtevo in na stroške stranke pomagala stranki z ustreznimi tehničnimi in organizacijskimi ukrepi, če je to mogoče, pri izpolnjevanju obveznosti stranke, da se odzove na zahteve za uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, določenih v 12. do 23. členu GDPR.

- 7.2. Družba Siemens Healthineers mora stranko nemudoma obvestiti o zahtevah posameznikov, na katere se nanašajo osebni podatki, za uveljavljanje svojih pravic iz 12. do 23. člena GDPR, zlasti kar zadeva pravico do dostopa do osebnih podatkov, pravico do popravka, pravico do izbrisa (»pravico biti pozabljen«), pravico do omejevanja obdelave, pravico do prenosljivosti podatkov, pravico do ugovora ali pravico, da niso predmet avtomatiziranega individualnega odločanja.

- 7.3. Ob upoštevanju narave obdelave, kot je opisana v glavni pogodbi in tej pogodbi o obdelavi osebnih podatkov, ter informacij, ki so na voljo pri družbi Siemens Healthineers, bo družba Siemens Healthineers stranki na njene stroške pomagala zagotoviti, da stranka sama izpolnjuje obveznosti v skladu z

32. členom GDPR (varnost obdelave);
33. členom GDPR (uradno obvestilo nadzornemu organu o kršitvi varstva osebnih podatkov):

v primeru kršitve varstva osebnih podatkov v zvezi z osebnimi podatki, ki jih obdeluje družba Siemens Healthineers, družba Siemens Healthineers obvesti stranko brez nepotrebnega odlašanja, potem ko je družba Siemens Healthineers izvedela za kršitev. Takšno obvestilo mora vsebovati vsaj:

- opis narave kršitve (po možnosti vključno s kategorijami in približnim številom zadevnih posameznikov, na katere se nanašajo osebni podatki, in zbirkami podatkov);
- podatke o kontaktni točki, na kateri je mogoče dobiti več informacij o kršitvi varstva osebnih podatkov;
- verjetne posledice kršitve in ukrepe, ki so bili sprejeti ali so predlagani za odpravo 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 zagotovijo brez nepotrebnega odlašanja, ko so na voljo.

34. členom GDPR (sporočilo posamezniku, na katerega se nanašajo osebni podatki, o kršitvi varstva osebnih podatkov);
35. členom GDPR (ocena učinka v zvezi z varstvom podatkov) in
36. členom GDPR (predhodno posvetovanje).

- 7.4. Če stranka potrebuje pomoč, lahko vzpostavi stik s pisarno pooblaščenca za varstvo podatkov družbe Siemens Healthineers na naslovu dataprivacy.func@siemens-healthineers.com.

8. Izbris

Po izbiri stranke se vsi osebni podatki stranke izbrišejo ali vrnejo po koncu opravljanja storitev, povezanih z obdelavo. Stranka s to pogodbo o obdelavi osebnih podatkov družbi Siemens Healthineers naroča, naj po zaključku opravljanja storitev v zvezi z obdelavo izbriše vse osebne podatke stranke in obstoječe kopije, razen če zakonodaja Evropske unije ali države članice zahteva hrambo osebnih podatkov. Do izbrisa podatkov mora družba Siemens Healthineers še naprej zagotavljati skladnost s to pogodbo o varstvu osebnih podatkov.

9. Pravice do obveščanja in revizije

- 9.1. V zvezi z obdelavo po glavni pogodbi bo družba Siemens Healthineers stranki na njeno pisno zahtevo dala na voljo vse

informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz 28. člena GDPR.

- 9.2. Družba Siemens Healthineers bo v zvezi z obdelavo po glavni pogodbi omogočila revizije, vključno z inšpekcijskimi pregledi (»revizije«), in sodelovala pri njih, da bi dokazala izpolnjevanje obveznosti iz 28. člena GDPR. Te revizije lahko izvede tudi neodvisna tretja oseba, ki jo pooblasti stranka, in sicer pod pogojem, da je ta revizor sprejemljiv za družbo Siemens Healthineers in zavezan k zaupnosti, ki ni manj stroga od tiste, ki velja za stranko po glavni pogodbi. Stranka mora zahtevati revizijo z razumnim predhodnim obvestilom družbi Siemens

Healthineers. Pred revizijo se stranki medsebojno dogovorita o obsegu, času in trajanju revizije. Stranka bo družbi Siemens Healthineers povrnila stroške za vse storitve, ki jih je družba Siemens Healthineers opravila v zvezi z revizijo, in to po veljavnih cenah storitev družbe Siemens Healthineers, ki se stranki zagotovijo na njeno zahtevo.

- 9.3. Stranka bo družbi Siemens Healthineers nemudoma predložila pisno poročilo z zaupnim povzetkom obsega in rezultatov revizije. Ne glede na to ima družba Siemens Healthineers pravico do uporabe poročila za lastne namene.

Priloga TOM:

Tehnični in organizacijski ukrepi (»TOM«) družbe Siemens Healthineers

1. Pseudonimizacija in šifriranje osebnih podatkov

Družba Siemens Healthineers ločuje osebne podatke od obdelanih podatkov tako, da obdelanih podatkov ni mogoče povezati z določeno ali določljivo osebo brez dodatnih informacij, ki so shranjene ločeno in varno. Družba Siemens Healthineers šifrira osebne podatke s simetričnimi ali asimetričnimi ključi.

2. Zaupnost, celovitost, razpoložljivost in odpornost sistemov in storitev

2.1 Družba Siemens Healthineers zaupnost in celovitost zagotavlja z naslednjimi ukrepi:

Nadzor dostopa:

Družba Siemens Healthineers varuje svoje stavbe z ustreznimi sistemi za nadzor dostopa, ki temeljijo na varnostni klasifikaciji stavb in ustrezno opredeljenem konceptu avtorizacije dostopa. Vse stavbe so zavarovane z ukrepi za nadzor dostopa z uporabo sistema čitalnikov kartic. Glede na varnostno kategorijo so premoženje, stavbe ali posamezna območja zavarovani z dodatnimi ukrepi. Ti vključujejo posebne profile za dostop, biometrične podatke, ploščice s številko PIN, ključne DES, ločilne ključavnice, videonadzor in varnostno osebje. Pravice dostopa za pooblaščen osebe se dodeljujejo individualno v skladu z opredeljenimi merili. To velja tudi za zunanje osebe.

Nadzor dostopa do sistema:

Dostop do sistemov za obdelavo podatkov se odobri le preverjenim uporabnikom na podlagi koncepta avtorizacije, ki temelji na vlogah, in sicer z uporabo naslednjih ukrepov: šifriranje podatkov, individualno dodeljevanje gesel (vsaj 8 znakov, redno samodejni iztek), identifikacijske kartice zaposlenih s šifriranjem PKI, z geslom zaščiteni ohranjevalniki zaslona v primeru neaktivnosti, sistemi za odkrivanje vdorov in sistemi za preprečevanje vdorov, redno posodabljanje protivirusnih programov in filtrov vohunske programske opreme v omrežju ter v posameznih osebnih računalnikih in mobilnih napravah.

Nadzor dostopa do podatkov:

Dostop do osebnih podatkov se odobri na podlagi koncepta avtorizacije, ki temelji na vlogah. Vzpostavljen je bil sistem za upravljanje uporabnikov, ki prikazuje podatkovno zbirko uporabnikov z njihovimi ustreznimi pooblastili in je na voljo centralno v omrežju, da ga lahko sistemi za obdelavo podatkov, ki zahtevajo dostop, poiščejo. Poleg tega šifriranje podatkov preprečuje nepooblaščen dostop do osebnih podatkov.

Nadzor prenosa podatkov:

Družba Siemens Healthineers varuje elektronske komunikacijske kanale z vzpostavitvijo zaprtih omrežij in postopki šifriranja podatkov. Ob fizičnem prenosu nosilcev podatkov se izvajajo preverljivi postopki prenosa, ki preprečujejo nepooblaščen dostop do podatkov ali logično izgubo. Nosilci podatkov se odstranijo v skladu s predpisi o varstvu podatkov.

2.2 Družba Siemens Healthineers stalno razpoložljivost in zanesljivost sistemov in storitev zagotavlja z naslednjimi ukrepi:

Družba Siemens Healthineers razpoložljivost in odpornost sistemov in storitev zagotavlja z izolacijo kritičnih IT-komponent in omrežnih komponent, z zagotavljanjem ustreznih rezervnih in redundantnih sistemov, uporabo sistemov za redundanco napajanja ter rednim testiranjem sistemov in storitev. Testni in delujoči sistemi so popolnoma ločeni.

3. Razpoložljivost in dostop do osebnih podatkov v primeru incidenta

Družba Siemens Healthineers razpoložljivost in dostop do osebnih podatkov v primeru fizičnega ali tehničnega incidenta obnovi z naslednjimi ukrepi:

Družba Siemens Healthineers hrani osebne podatke v sistemih RAID in integrira redundantne sisteme v skladu z varnostno oznako. Družba Siemens Healthineers uporablja sisteme za neprekinjeno napajanje (npr. UPS, baterije, generatorje), da zagotovi oskrbo z električno energijo v podatkovnih centrih.

Podatkovne zbirke ali podatkovni centri so zrcaljeni na različnih fizičnih lokacijah.

Na voljo je celovit pisni načrt za ravnanje v izrednih razmerah. Postopki in sistemi za ukrepanje v izrednih razmerah se redno pregledujejo.

4. Nadzorni postopki za zagotavljanje varnosti obdelave

Družba Siemens Healthineers vzdržuje nadzorne postopke na podlagi obvladovanja tveganj, ob upoštevanju osnovnih katalogov zaščite IT Zveznega urada za informacijsko varnost (BSI) in zahtev standarda ISO/IEC 27001 za redno pregledovanje, ocenjevanje in vrednotenje učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave. S tem je zagotovljena zaščita ustreznih informacij, aplikacij (vključno z metodami testiranja kakovosti in varnosti), operativnih okolij (npr. s spremljanjem omrežja v zvezi s škodljivimi vplivi) in tehničnega izvajanja konceptov zaščite (npr. z analizami ranljivosti). S sistematičnim odkrivanjem in odpravljanjem šibkih točk se zaščitni ukrepi nenehno preverjajo in izboljšujejo.

5. Kadrovske ukrepi

Družba Siemens Healthineers izda pisna navodila za delo in redno usposablja osebje, ki ima dostop do osebnih podatkov, da zagotovi obdelavo osebnih podatkov, ki bo v skladu z zakonom, to pogodbo o obdelavi osebnih podatkov in s povezanimi navodili stranke, vključno s tukaj opisanimi tehničnimi in organizacijskimi ukrepi.