Zmluva o spracúvaní osobných údajov podľa čl. 28 GDPR (ďalej len „DPA“)

(Verzia: 30.03.2026)

Táto DPA dopĺňa a špecifikuje povinnosti pri ochrane osobných údajov podľa zmluvy uzatvorenej medzi Zmluvnými stranami. Táto DPA sa vzťahuje na všetky činnosti súvisiace s hlavnou zmluvou, v rámci ktorých zamestnanci Siemens Healthineers alebo tretie osoby zazmluvnené Siemens Healthineers spracúvajú osobné údaje Zákazníka alebo jeho klientov a iných osôb.

0. Výklad

0.1. Ak táto DPA používa pojmy definované vo Všeobecnom nariadení o ochrane údajov (ďalej len „GDPR“), tieto pojmy majú rovnaký význam ako v GDPR.

0.2. Túto DPA treba čítať a vykladať v súlade s ustanoveniami GDPR.

0.3. Táto DPA sa nesmie vykladať spôsobom, ktorý by bol v rozpore s právami a povinnosťami stanovenými v GDPR alebo spôsobom, ktorý by poškodzoval základné práva alebo slobody dotknutých osôb.

1. Predmet, povaha, účel a doba spracúvania

1.1. Táto DPA dopĺňa hlavnú zmluvu uzatvorenú medzi Siemens Healthineers a Zákazníkom. Vzťahuje sa na spracúvanie osobných údajov spoločnosťou Siemens Healthineers („Sprostredkovateľ“) v mene Zákazníka („Prevádzkovateľ“) podľa hlavnej zmluvy a stanovuje povinnosti zmluvných strán týkajúce sa ochrany osobných údajov. Konkrétny popis predmetu, povahy, účelu a trvania spracúvania osobných údajov Siemens Healthineers pre Zákazníka je uvedený v hlavnej zmluve.

1.2. Povaha a účel spracúvania: Siemens Healthineers spracúva osobné údaje v rozsahu potrebnom na poskytovanie služieb špecifikovaných a dohodnutých v hlavnej zmluve. Siemens Healthineers nesmie spracúvať osobné údaje na iné účely.

1.3. Siemens Healthineers a Zákazník sú zodpovední za dodržiavanie príslušných predpisov o ochrane osobných údajov. Zákazník je samostatne zodpovedný za spôsob, akým získa osobné údaje a Zákazník poskytne Siemens Healthineers iba také osobné údaje, na ktorých poskytnutie má oprávnenie a v prípade, ak má právo na ich spracúvanie.

1.4. Doba spracúvania zodpovedá trvaniu hlavnej zmluvy.

2. Typ osobných údajov a kategórie dotknutých osôb

V nadväznosti na ustanovenia hlavnej zmluvy sú kategóriami dotknutých osôb najmä zamestnanci, pacienti, kontaktné osoby Zákazníka a zmluvní partneri Zákazníka. Medzi typy osobných údajov zahrnuté do spracúvania patria najmä kontaktné informácie, identifikátory, údaje o polohe, finančné informácie a citlivé údaje ako zdravotné informácie (údaje týkajúce sa zdravia), genetické údaje a biometrické údaje.

3. Pokyny

3.1. Siemens Healthineers spracúva osobné údaje iba na základe zdokumentovaných pokynov Zákazníka. Táto DPA a hlavná zmluva predstavujú úplné a konečné zdokumentované pokyny pre Siemens Healthineers na spracúvanie osobných údajov.

3.2. Akékoľvek dodatočné alebo alternatívne pokyny musí Zákazník vydať písomne a budú záväzné iba po písomnom potvrdení Siemens Healthineers. Siemens Healthineers bude informovať Zákazníka, ak podľa jej názoru pokyn porušuje GDPR alebo predpisy o ochrane osobných údajov vzťahujúce sa na Siemens Healthineers ako na sprostredkovateľa osobných údajov. Siemens Healthineers nemá povinnosť vykonávať komplexné právne posúdenie pokynov alebo dodržiavať pokyny, ktoré sú zákonom zakázané.

3.3. Zákazník je povinný znášať všetky dodatočné náklady vynaložené Siemens Healthineers ako výsledok dodatočného alebo alternatívneho pokynu, pokiaľ pokyn nie je nevyhnutný na splnenie zákonných požiadaviek platných pre Siemens Healthineers.

4. Dôvernosť informácií

Siemens Healthineers je povinná poskytnúť svojim zamestnancom prístup k spracúvaným osobným údajom len v rozsahu nevyhnutne potrebnom na realizáciu, riadenie a monitorovanie hlavnej zmluvy. Siemens Healthineers zabezpečuje, že osoby oprávnené spracúvať osobné údaje sú zmluvne alebo na základe zákonných predpisov viazané povinnosťou mlčanlivosti.

5. Bezpečnosť spracúvania

5.1. Siemens Healthineers vykoná všetky požadované opatrenia podľa článku 32 GDPR.

5.2. Zohľadňujúc stav najnovších poznatkov, náklady na implementáciu opatrení, povahu, rozsah, kontext a účely spracúvania, ako aj na rôzny stupeň pravdepodobnosti a závažnosti rizika pre práva a slobody fyzických osôb, tiež so zreteľom na riziká, ktoré sú spojené so spracúvaním, najmä s náhodným alebo nezákonným zničením, stratou, zmenou, neoprávneným zverejnením alebo prístupom k prenesenému, uloženému alebo inému spôsobom spracúvanému osobnému údajom, Siemens Healthineers prijme technické a organizačné opatrenia tak ako sú uvedené v Prílohe TAOO.

5.3. Zákazník a Siemens Healthineers sa zhodli, že implementácia týchto technických a organizačných opatrení uvedených v Prílohe TAOO zabezpečuje primeranú úroveň bezpečnosti v súlade s GDPR a poskytuje dostatočné záruky na ochranu práv dotknutej osoby.

5.4. Technické a organizačné opatrenia popísané v Prílohe TAOO podliehajú technickému pokroku a ďalšiemu vývoju a môžu byť upravené Siemens Healthineers, ak je to vhodné, za predpokladu, že takéto prispôsobenie nebude mať za následok nižšiu úroveň ochrany, než je tá, ktorá je uvedená v Prílohe TAOO.

6. Ďalší sprostredkovatelia

6.1. Siemens Healthineers nezadá subdodávateľom, resp. ďalším sprostredkovateľom, žiadnu zo svojich vykonávaných spracovateľských činností bez predchádzajúceho povolenia Zákazníka. Ak Siemens Healthineers zadá svoje spracovateľské činnosti subdodávateľom, resp. ďalším sprostredkovateľom, s povolením Zákazníka, subdodávatelia, resp. ďalší sprostredkovatelia, môžu spracúvať osobné údaje iba na účely vykonávania činností, na ktoré boli tieto osobné údaje Siemens Healthineers poskytnuté, a je zakázané spracúvať osobné údaje na iné účely.

Každý subdodávateľ, resp. ďalší sprostredkovateľ, sa zaväzuje na základe zmluvy, ktorá v podstate ukladá subdodávateľovi, resp. ďalšiemu sprostredkovateľovi, v podstate rovnaké povinnosti v oblasti ochrany osobných údajov, ako sú tie, ktoré sú uložené Siemens Healthineers v súlade s touto DPA, najmä takáto zmluva musí poskytovať dostatočné záruky, s účelom vykonávať vhodné technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky GDPR, zabezpečovať ochranu práv dotknutých osôb, viesť záznamy o prenosoch údajov a dokumentovať vhodné záruky. Na žiadosť Zákazníka Siemens Healthineers poskytne Zákazníkovi kópiu takejto zmluvy so subdodávateľom, resp. ďalším sprostredkovateľom, a všetkých jej následných dodatkov. V rozsahu potrebnom na ochranu

obchodných tajomstiev alebo iných dôverných informácií vrátane osobných údajov môže Siemens Healthineers upraviť text zmluvy pred zdieľaním kópie.

6.2. Zoznam ďalších sprostredkovateľov Siemens Healthineers je k dispozícii na https://fleet.siemens-healthineers.com/welcome. Siemens Healthineers si vyhradzuje právo z času na čas aktualizovať túto URL (webovú stránku). Zákazník týmto udeľuje Siemens Healthineers všeobecné povolenie, aby zapojila subjekty uvedené v tomto zozname ako ďalších sprostredkovateľov.

Zákazník je povinný sa zaregistrovať na uvedenej webovej stránke, aby mohol byť informovaný o ďalších sprostredkovateľoch, a o akýchkoľvek plánovaných zmenách vo používaní, resp. výmene ďalších sprostredkovateľov. Siemens Healthineers je zodpovedná za zhromažďovanie relevantných informácií od ďalších sprostredkovateľov a udržiavanie tohto zoznamu v aktuálnom stave.

Zapojenie ďalšieho sprostredkovateľa alebo nahradenie ďalšieho sprostredkovateľa iným ďalším sprostredkovateľom sa považuje za schválené zo strany Zákazníka, ak o tom Siemens Healthineers Zákazníka vopred informuje a Zákazník proti tomu nevznesie písomnú námietku, a to ani v elektronickej podobe, do 30 dní od oznámenia takejto informácie.

6.3. V prípade námietok Zákazník oznámi Siemens Healthineers

podrobnosti o dôvodoch námietky.

Po obdržaní námietky môže Siemens Healthineers podľa vlastného uváženia

a. namiesto zamietnutého ďalšieho sprostredkovateľa navrhnúť iného ďalšieho sprostredkovateľa; alebo

b. podniknúť kroky na vyriešenie výhrad vznesených Zákazníkom, v ktorých dôsledku sa namietané výhrady odstránia.

6.4. Ak ani pri rozumnom posúdení nemožno využiť možnosti podľa tohto článku 6 ods. 3 a. a b. alebo ak namietané výhrady nemožno odstrániť inak, môže Siemens Healthineers ukončiť hlavnú zmluvu úplne alebo čiastočne bez výpovednej lehoty, napr. ak námietka Zákazníka podstatne sťažuje alebo znemožňuje Siemens Healthineers plniť jej zmluvné záväzky.

6.5. Počínajúc plánovaným dátumom začatia plnenia namietaného ďalšieho sprostredkovateľa bude pozastavená platnosť všetkých dohôd o dobách odozvy alebo dostupnosti a akékoľvek nároky na náhradu škody uplatnenú namiesto plnenia, nároky na náhradu škody z dôvodu omeškania, alebo dohodnuté paušálne náhrady škody alebo zmluvné pokuty týkajúce sa Siemens Healthineers sa nebudú uplatňovať. Ak dôjde k čiastočnému ukončeniu povinnosti poskytovať plnenie Siemens Healthineers, odmena za časť služieb resp. plnenia, ktorá nie je dotknutá čiastočným ukončením, sa určí na základe štandardného cenníka Siemens Healthineers pre tieto služby resp. plnenia.

6.6. Ak ďalší sprostredkovateľ nesplní svoje povinnosti v oblasti ochrany osobných údajov, Siemens Healthineers v súlade s ustanoveniami o zodpovednosti v hlavnej zmluve, zostáva plne zodpovedná voči Zákazníkovi za plnenie povinností ďalšieho sprostredkovateľa. Siemens Healthineers nenesie zodpovednosť za škody a nároky vyplývajúce z dodatočných alebo alternatívnych pokynov Zákazníka podľa článku 3 ods. 2 tejto DPA.

6.7. V prípade, že Siemens Healthineers zapojí ďalšieho sprostredkovateľa v tretej krajine (mimo EÚ/EHP), Siemens Healthineers použije mechanizmy prenosu údajov v súlade s článkami 44 a nasl. GDPR.

6.8. Zákazník súhlasí s tým, že ak je v súlade s týmto článkom 6 zapojený ďalší sprostredkovateľ na vykonávanie konkrétnych spracovateľských činností (v mene Zákazníka) a tieto činnosti spracúvania zahŕňajú prenos osobných údajov v zmysle článkov 44 a ods. nasl. GDPR, súlad s článkami 44 a nasl. GDPR možno zabezpečiť buď použitím štandardných doložiek o ochrane údajov prijatých Komisiou v súlade s článkom 46 ods. 2 GDPR za predpokladu, že sú splnené podmienky na použitie týchto štandardných doložiek o ochrane údajov, alebo použitím iných vhodných záruk v súlade s článkom 46 GDPR.

7. Poskytovanie pomoci

7.1. Po zohľadnení povahy spracúvania údajov uvedeného v hlavnej zmluve a v tejto DPA bude Siemens Healthineers Zákazníkovi pomáhať, na jeho žiadosť a na jeho náklady, v čo najväčšej miere vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby ustanovených v článkoch 12 až 23 GDPR.

7.2. Siemens Healthineers bez zbytočného odkladu informuje Zákazníka o žiadostiach dotknutých osôb, ktorými uplatňujú svoje práva podľa článkov 12 až 23 GDPR, najmä pokiaľ ide o právo na prístup k osobným údajom, právo na opravu, právo na vymazanie (právo „na zabudnutie“), právo na obmedzenie spracúvania, právo na prenosnosť údajov, právo namietať alebo právo nepodliehať automatizovanému individuálnemu rozhodovaniu.

7.3. Po zohľadnení povahy spracúvania uvedenej v hlavnej zmluve a v tejto DPA a informácií, ktoré má Siemens Healthineers k dispozícii, Siemens Healthineers poskytne Zákazníkovi na jeho náklady pomoc zabezpečiť súlad Zákazníka s jeho povinnosťami podľa

a. článku 32 GDPR (bezpečnosť spracúvania);

b. článku 33 GDPR (oznámenie porušenia ochrany osobných údajov dozornému orgánu);

V prípade porušenia ochrany osobných údajov týkajúcich sa osobných údajov spracúvaných Siemens Healthineers, Siemens Healthineers informuje Zákazníka bez zbytočného odkladu po tom, čo sa Siemens Healthineers o porušení dozvedela. Takéto oznámenie obsahuje aspoň:

(i) opis povahy porušenia (ak je to možné, vrátane kategórií a približného počtu dotknutých osôb a dotknutých záznamov resp. osobných údajov);

(ii) údaje o kontaktnom mieste, kde možno získať viac informácií o porušení ochrany osobných údajov;

(iii) jeho pravdepodobné dôsledky a prijaté alebo navrhované opatrenia na riešenie porušenia ochrany osobných údajov vrátane zmiernenia jeho možných nepriaznivých účinkov.

Ak a pokiaľ nie je možné poskytnúť všetky tieto informácie súčasne, prvé oznámenie obsahuje informácie, ktoré sú v tom čase dostupné, a ďalšie informácie, keď budú dostupné, sa následne poskytnú bez zbytočného odkladu.

c. článku 34 GDPR (oznámenie porušenia ochrany osobných údajov dotknutej osobe);

d. článku 35 GDPR (posúdenie vplyvu na ochranu údajov); a

e. článku 36 GDPR (predchádzajúca konzultácia).

7.4. V prípade, ak Zákazník potrebuje pomoc, môže kontaktovať Kanceláriu Zodpovednej osoby Siemens Healthineers na adrese dataprivacy.func@siemens-healthineers.com.

8. Vymazanie

Na základe voľby Zákazníka musia byť všetky osobné údaje Zákazníka vymazané alebo vrátené po ukončení poskytovania služieb, ktorých sa spracúvanie týka. Zákazník týmto dáva pokyn Siemens Healthineers vymazať všetky osobné údaje Zákazníka po skončení poskytovania služieb súvisiacich so spracúvaním a vymazať existujúce kópie, pokiaľ právo Únie alebo členského štátu nevyžaduje uchovávanie osobných údajov. Až do vymazania údajov bude Siemens Healthineers naďalej zabezpečovať súlad s touto DPA.

9. Právo na informácie a na audit

9.1. Pokiaľ ide o spracúvanie údajov na základe hlavnej zmluvy, Siemens Healthineers na základe písomnej žiadosti Zákazníka sprístupní Zákazníkovi všetky informácie potrebné na preukázanie súladu s povinnosťami stanovenými v článku 28 GDPR.

9.2. Siemens Healthineers umožní výkon Zákazníckych auditov a prispeje ich k vykonaniu, vrátane kontrol (ďalej len „audity“), týkajúcich sa spracúvania osobných údajov na základe hlavnej zmluvy, na preukázanie súladu s povinnosťami stanovenými v článku 28 GDPR. Tieto audity môže vykonávať aj nezávislý audítor tretej strany, ktorý má poverenie Zákazníka, za predpokladu, že tento audítor je pre Siemens Healthineers prijateľný a že je viazaný povinnosťou zachovávať mlčanlivosť minimálne v rozsahu ako Zákazník na základe hlavnej zmluvy. Pri žiadosti o audit Zákazník primerane včas oznámi túto skutočnosť Siemens Healthineers. Pred auditom sa zmluvné strany vzájomne dohodnú na rozsahu, načasovaní a trvaní auditu. Zákazník uhradí odplatu Siemens Healthineers za všetky služby, ktoré Siemens Healthineers poskytla v súvislosti s auditom, a to za ceny podľa aktuálneho sadzobníka služieb Siemens Healthineers, ktorý bude na požiadanie k dispozícii Zákazníkovi.

9.3. Zákazník bezodkladne poskytne Siemens Healthineers písomnú správu obsahujúcu dôverné zhrnutie rozsahu a výsledkov auditu. Bez ohľadu na uvedené, je Siemens Healthineers oprávnená bez akýchkoľvek obmedzení používať túto správu na vlastné účely.

Príloha TAOO:
Technické a organizačné opatrenia ("TAOO") Siemens Healthineers

1. Pseudonymizácia a šifrovanie osobných údajov

Siemens Healthineers oddeľuje osobné údaje od spracúvaných údajov, takže nie je možné prepojiť spracúvané údaje s identifikovanou alebo identifikovateľnou osobou bez ďalších informácií, ktoré sú uložené samostatne a bezpečne. Siemens Healthineers šifruje osobné údaje pomocou symetrických a asymetrických kľúčov.

2. Dôvernosť,integrita, dostupnosť a odolnosť systémov a služieb

2.1 Siemens Healthineers zabezpečuje dôvernosť a integritu tým, že prijme nasledujúce opatrenia:

Kontrola prístupu:

Siemens Healthineers chráni svoje budovy pomocou vhodných systémov kontroly prístupu založených na bezpečnostnej klasifikácii budov a primerane definovanej koncepcii autorizovaného prístupu. Všetky budovy sú zabezpečené opatreniami na kontrolu prístupu pomocou systému čítačky kariet. V závislosti od kategórie zabezpečenia sú nehnuteľnosti, budovy alebo jednotlivé oblasti zabezpečené dodatočnými opatreniami. Patria medzi ne špeciálne prístupové profily, biometrické prvky, pinové podložky, DES dongle, oddeľovacie zámky, kamerový systém a bezpečnostný služba. Prístupové práva oprávnených osôb sa udeľujú individuálne podľa definovaných kritérií. To platí aj pre externé osoby.

Ovládanie prístupu k systémom:

Prístup k systémom na spracúvanie údajov sa poskytuje iba autentifikovaným používateľom na základe koncepcie autorizácie založenej na rolách s použitím nasledujúcich opatrení: Šifrovanie dát, individuálne priradenie hesla (minimálne 8 znakov, pravidelné automatické vypršanie platnosti), identifikačné karty zamestnancov s šifrovaním PKI, chránené šetriče obrazovky v prípade nečinnosti, systémy detekcie vniknutia a systémy na prevenciu narušenia, pravidelne aktualizované antivírusové a spyware filtre v sieti a na jednotlivých počítačoch a mobilných zariadeniach.

Ovládanie prístupu k údajom:

Prístup k osobným údajom je udelený na základe koncepcie autorizácie povoľovania založenej na jednotlivých rolách. Bol vytvorený systém správy používateľov, ktorý mapuje databázu používateľov s príslušnými oprávneniami a je centrálne dostupný v sieti na vyhľadanie prostredníctvom požiadavky na systémy spracúvania údajov. Okrem toho šifrovanie údajov zabraňuje neoprávnenému prístupu k osobným údajom.

Ovládanie prenosu údajov:

Siemens Healthineers zabezpečuje elektronické komunikačné kanály nastavením uzavretých sietí a šifrovacích postupov. Ak dôjde k fyzickému prenosu dátových nosičov, implementujú sa overiteľné prepravné procesy, ktoré zabraňujú neoprávnenému prístupu k dátam alebo logickej strate. Dátové nosiče sa likvidujú v súlade s predpismi o ochrane údajov.

2.2 Siemens Healthineers zabezpečuje trvalú dostupnosť a spoľahlivosť systémov a služieb tým, že prijíma tieto opatrenia:

Siemens Healthineers zabezpečuje dostupnosť a odolnosť

systémov a služieb izoláciou kritických IT a sieťových komponentov, poskytovaním adekvátnych zálohových a

redundantných systémov, využívaním systémov redundancie energie a pravidelným testovaním systémov a služieb. Testovacie a živé systémy sú udržiavané úplne oddelené.

3. Dostupnosť a prístup k osobným údajom v prípade incident

Siemens Healthineers obnoví dostupnosť a prístup k osobným údajom v prípade fyzickej alebo technickej udalosti tým, že prijme tieto opatrenia:

Siemens Healthineers uchováva osobné údaje v systémoch RAID a integruje redundantné systémy podľa bezpečnostného označenia. Siemens Healthineers používa systémy na neprerušiteľné napájanie (napríklad UPS, batérie, generátory) na zabezpečenie napájania dátových centier.

Databázy alebo dátové centrá sa odzrkadľujú na rôznych

miestach.

Komplexný písomný núdzový plán je k dispozícii. Núdzové procesy a systémy sa pravidelne prehodnocujú.

4. Kontrolné postupy na zaistenie bezpečnosti spracúvania

Siemens Healthineers udržiava kontrolný postup založený na prístupe založenom na riadení rizík, pričom zohľadňuje základné katalógy ochrany IT od spolkového úradu pre informačnú bezpečnosť (BSI) a požiadavky ISO /IEC 27001 na pravidelné preskúmanie, hodnotenie a vyhodnocovanie účinnosti technických a organizačných opatrení na zabezpečenie bezpečnosti spracúvania. Tým sa zabezpečuje ochrana relevantných informácií, aplikácií (vrátane metód testovania kvality a bezpečnosti), prevádzkových prostredí (napríklad monitorovaním siete proti škodlivým účinkom) a technickej implementácie koncepcií ochrany (napríklad pomocou analýz zraniteľnosti). Systematickým zisťovaním a odstraňovaním slabých miest sa ochranné opatrenia neustále spochybňujú a zlepšujú.

5. Personálne opatrenia

Siemens Healthineers vydáva písomné pracovné pokyny a pravidelne zaškoľuje zamestnancov, ktorí majú prístup k osobným údajom, aby zabezpečil, že osobné údaje budú spracúvané iba v súlade s právnymi predpismi, touto DPA a súvisiacimi pokynmi Zákazníka vrátane technických a organizačných opatrení opísaných v tejto Prílohe TaOO.