

Prohlášení o ochraně údajů v produktu MEDICUS

CompuGroup Medical Česká republika s.r.o.



1. Organizace ochrany údajů a převzetí odpovědnosti za ochranu údajů

CompuGroup Medical Česká republika s.r.o. (dále jen CGM ČR) považuje ochranu osobních údajů a zodpovědné nakládání s nimi za základní princip. CGM ČR se zavazuje k přísnému dodržování všech příslušných právních předpisů a norem týkajících se ukládání a zpracování osobních údajů.

Společnost CGM SE implementovala centrální systém řízení ochrany dat, který zajišťující trvalou a vysokou úroveň ochrany osobních údajů ve všech společnostech CGM v souladu s příslušnými právními předpisy.

Toto prohlášení o ochraně dat slouží k naplnění zákonem stanovené informační povinnosti poskytování informací o nakládání s daty v rámci CGM. Toto prohlášení o ochraně dat se týká výslovně MEDICUS

Přístup k nejnovější verzi tohoto prohlášení o ochraně dat budete mít kdykoliv v produktu MEDICUS a na webových stránkách společnosti CGM ČR v následujícím odkazu:

http://filesrv.compugroup.cz/navody/gdpr/DataProtectionStatement_MEDICUS.pdf

2. MEDICUS

MEDICUS je lékařský systém vhodný pro všechny běžné formy lékařských ordinací v ambulantním sektoru a podporuje postupy při dodržování zásad vyplývajících z právních požadavků, strukturované dokumentace, řízení ordinace, fakturace, vydávání lékařských předpisů a dalších požadavků. Systém je možné rozšiřovat pomocí volitelných modulárních doplňků.

MEDICUS poskytuje autorizovaným osobám management uživatelských práv, aby přístup k systému (a datům uloženým v systému) byl povolen pouze oprávněným osobám. Pomocí uživatelských práv je řízen také přístup k modulárním doplňkům systému.

Mimo řízení přístupu uživatelů poskytuje MEDICUS také kontrolu přístupu uživatelů (například čtení a zápis) k záznamům uložených v rámci tohoto systému.

3. Zpracování osobních údajů společností CGM ČR

Osobní data jsou jakékoliv informace spojené s identifikovanou nebo identifikovatelnou fyzickou osobou. Identifikovatelnou fyzickou osobou je osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na jméno, identifikační číslo, lokalizační údaje, online identifikátor nebo s odkazem na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychologické, ekonomické, kulturní nebo sociální identity této fyzické osoby

Při používání výše uvedeného produktu a/nebo služeb jsou na serverech CGM ČR ukládány pouze data z technických operací.

Těmito "technickými operacemi" jsou on-line služby provozované na serverech CGM ČR pro zajištění smluvně garantovaných služeb, jako je například:

- distribuce aktualizací systému MEDICUS provozovaného v ordinaci,
- distribuce obecně platných číselníků a katalogů,
- distribuce aktuálních licenčních klíčů k zákazníkům

Při používání těchto služeb budou dočasně na serverech CGM uložena data, která jsou nezbytná k zajištění integrity a bezpečnosti provozu systému MEDICUS:

- IP adresy klientských počítačů,
- datum a čas přístupu,
- identifikátor licence systému MEDICUS (sérové číslo nebo jiný identifikační údaj, na jehož základě jsou systémy CGM ČR schopny identifikovat a autorizovat nárok ordinace na využití těchto služeb),
- aktuální verze systému, jednotlivých samostatných komponent, popřípadě číselníků či katalogů instalovaných
- informace o kritických chybách systému MEDICUS provozované v ordinaci

CGM shromažďuje data z technických operací pouze za tímto účelem.

4. Zpracování osobních údajů ambulantním systémem MEDICUS na serveru Vaší lékařské ordinace

- **Kmenová data pracovišť zdravotnického zařízení a jejich zaměstnanců**
- **Údaje pacientů**
 - Osobní údaje
 - Zvláštní kategorie osobních údajů (citlivé údaje)

Údaje o zdravotním zařízení, přihlašovací údaje, údaje o zaměstnancích a pacientech jsou uloženy na Vašem serveru a zůstávají majetkem zařízení i po ukončení smlouvy. Další zacházení s těmito daty je v plně v režii zdravotnického zařízení. Máte právo provádět opravy dat, právo k omezení zpracování a právo k vymazání těchto dat umístěných na Vašem serveru.

Ukládání a zpracování osobních údajů zpřístupněných společnosti CGM během obchodních a smluvních vztahů slouží a je omezeno na účely plnění smlouvy, zejména ke zpracování objednávek a k zákaznické podpoře. Data nebudou předána nebo prodána žádné třetí straně, pokud to není nezbytné ke splnění smluvních závazků nebo pokud to není výslovně povoleno prohlášením o souhlasu. Toto může být například důležité pro společnost CGM k předání adresy a objednacích údajů prodejnímu a servisnímu partnerovi, pokud byla vystavena objednávka.

4.1 Kmenová data lékařské praxe a jejich zaměstnanců

Kmenová data Vaší ordinace a zaměstnanců ordinace jsou v systému MEDICUS ukládána z důvodu souladu s právními požadavky na činnosti prováděné v tomto systému a jeho modulech (vedení zdravotnické dokumentace, řízení přístupu k ní, vyúčtování zdravotní péče, vykazování statistik, vytváření elektronické preskripce a podobně). Povinná kmenová data v MEDICUS jsou odpovídajícím způsobem označena. Kmenová data lékařské ordinace a jejich zaměstnanců zahrnují:

- Název a adresa ordinace
- Typ ordinace
- IČO, DIČ a IČZ subjektu (ordinace)
Údaje o pracovištích zdravotnického zařízení, zejména odbornosti, IČP, lokality, ordinační doby, poskytované služby
- Data související s lékařem/Provozovatelem lékařské praxe
 - Oslovení/Titul
 - Křestní jméno/Příjmení
- Informace o pracovnících ordinace (zaměstnanci, popřípadě majitel ordinace):

Prohlášení o ochraně údajů v produktu MEDICUS

CompuGroup Medical Česká republika s.r.o.



- Příjmení, křestní jméno,
- Uživatelské jméno/bezpečný hash hesla
- Kontaktní údaje (telefon, e-mail adresa, jiné adresy a identifikátory pro elektronickou komunikaci)
- U lékařů pak odbornost lékaře, evidenční číslo lékaře v ČLK
- Osobní přístupové údaje do systémů třetích stran. Tyto jsou v systému ukládány v šifrované podobě, aby k nim neměl přístup ani správce systému. Jde například o přístupové údaje do Centrálního úložiště elektronické preskripce (SÚKL) nebo přístupy pro předávání dávek do zdravotních pojišťoven.
- Otisk osobního kvalifikovaného certifikátu

Kmenová data v jednotlivých funkcích a modulech systému využívána automaticky.

Při výkonu vybraných činností uživatele v systému MEDICUS dochází k přenosu dat ordinace (a jejich zaměstnanců). Pokud je prováděn přenos dat nad rámec povinností daných legislativou (například součástí zdravotnické dokumentace musí být jméno a příjmení pracovníka), musí být přenos proveden na základě předchozího prohlášením o souhlasu.

Opravy, omezení zpracování nebo mazání těchto dat je plně v pravomoci zdravotnického zařízení v souladu s právními předpisy.

4.2 Údaje pacientů

V rámci používání MEDICUS dochází k zpracování osobních údajů pacientů a údajů zvláštní kategorie.

Kategorie osobních údajů a účel zpracování osobních údajů v systému MEDICUS:

- osobní údaje a údaje o zdravotním stavu (včetně rodinné a sociální anamnézy, v případě potřeby etnický původ a genetické údaje) za účelem řádného vedení zdravotnické dokumentace k poskytování zdravotní péči, plnění povinností při poskytování zdravotních služeb
- osobní údaje a informace o pojištění pacienta u ZP za účelem vyúčtování zdravotní péče
- osobní údaje pacientů a kontaktní údaje (e-mail, telefon), termín a důvod objednávky za účelem zefektivnění přijímání pacientů v ordinaci a využití pracovní doby ordinace.
- daňové doklady a na nich uvedené osobní údaje pacientů z důvodu řádného vedení daňových dokladů

V systému mohou být nad rámec těchto základních účelů zpracovávány i jiné údaje pacientů. Zákonost těchto zpracování, popřípadě nutnost souhlasu pacientů s konkrétním účelem zpracování je zodpovědností správce osobních údajů.

Údaje o pacientech nejsou v informačních systémech generovány automaticky, ale jsou shromažďovány a vkládány do informačního systému v rámci dokumentace péče o pacienta personálem zdravotnického zařízení.

Evidovanými osobními údaji jsou:

- Osobní údaje (křestní jméno, příjmení, titul před nebo za jménem, rodné příjmení, datum a místo narození, věk, pohlaví, rodné číslo, státní občanství, číslo občanského průkazu, stav)
- Adresa trvalá a kontaktní (Ulice, číslo domu, poštovní směrovací číslo, město, země)
- Telefonní číslo, e-mailová adresa
- Informace o plátcí zdravotní péče a typu pojištění (zdravotní pojišťovna, číslo pojištěnce, soukromé zdravotní pojištění)
- Praktický lékař, ošetřující lékař, v případě předání pacienta do péče dalším lékařem i Doporučující lékař
- Údaje o zaměstnání (povolání, zaměstnavatel, adresa)
- Informace o osobě blízké (jméno, adresa, telefonní kontakt)

Citlivá data: Údaje o zdravotní péči jsou speciální kategorií osobních údajů a jsou předmětem vyšší ochrany v rámci obecného nařízení o ochraně osobních údajů.

Integrace dat do lékařských záznamů pacienta je dána zákonem stanovenou povinností ošetřujícího lékaře zaznamenávat a dokumentovat veškerá vyšetření a postupy léčby a jednotlivé výsledky podstatné pro současnou a budoucí léčbu pacienta.

Tato data zahrnují:

- Anamnézy
- Alergie
- Výška, hmotnost, krevní skupina
- Diagnózy
- Vyšetření
- Výsledky vyšetření
- Nálezy
- Terapeutická ošetření a jejich výsledky
- Operační zákroky a jejich výsledky
- Medikace pacienta
- Lékařské a ošetřovatelské zprávy, další zdravotnická dokumentace

Dle přístupových práv a nastavení systému lze provádět změny v záznamech pacienta a nahlížet na ně. Mazání dat musí být prováděno s ohledem na odpovídající legislativu a povinnosti lékaře. O přístupech k osobním údajům uloženým v systému jsou vedeny auditní záznamy. Systém, v souladu s požadavky GDPR, umožňuje lékařům ordinace vyhovět pacientům při uplatnění práva na přístup subjektu k osobním údajům

5. Přenos dat / transfer

Elektronický přenos dat je uskutečňován v MEDICUS pouze s vědomím uživatele na základě interakce s uživatelem nebo po udělení souhlasu.

Přenos dat může lékař provádět na základě právních požadavků, smluvních závazků nebo po předchozím souhlasu subjektů údajů.

Systém MEDICUS umožňuje následující přenosy dat:

5.1. Export dávek pro pojišťovnu

Export dávek do souborového systému, popřípadě pro uživatele modulu eDávky i vlastní přenos dávek na servery pojišťovny.

Přenos dat je založen na právních požadavcích.

5.2. Export zdravotnické dokumentace ve formátu DS MZ ČR (DASTA)

Export zdravotnické dokumentace ve formátu DASTA - pomocí tohoto exportu lze přenášet:

- lékařské zprávy a dekurzy (denní záznamy pacienta)
- výpis ze zdravotnické dokumentace pacienta
- žádanky na vyšetření (laboratorní, radiologická, patologická, vyšetření u ambulantních specialistů)

V základním systému MEDICUS lze exportovat potřebná data do souborového systému a vlastní přenos si lékař zajistí sám.

Uživatelé nadstavbového komunikačního modulu MEDICAL NET mají tímto modulem zajištěn bezpečný šifrovaný přenos až do ordinace příjemce dat.

Zákazník je povinen zajistit a odpovídá za to, aby přenos dat byl používán v souladu s platnou legislativou.

5.3. Přenos dat pacientům prostřednictvím modulu CGM LIFE eSERVICES

Pomocí nadstavbového komunikačního modulu CGM LIFE eSERVICES systému MEDICUS mohou uživatelé přenášet data bezpečným způsobem (šifrovaně) svým pacientům.

V tomto případě je přenos dat založený na předchozím souhlasu pacienta.

5.4. Přenos dat prostřednictvím modulu CGM-esky

Pomocí modulu CGM-esky systému MEDICUS mohou uživatelé posílat svým pacientům SMS zprávy. Přenášet data bezpečným způsobem (šifrovaně) svým pacientům.

Zákazník je povinen zajistit a odpovídat za to, aby přenos dat byl používán v souladu s platnou legislativou. Pokud uživatel používá zaslání SMS zpráv například k marketingovým účelům ordinace, musí být přenos dat založen na předchozím souhlasu pacientů.

6. Závazek o zachování důvěrnosti, školení o ochraně dat

Závazek o mlčenlivosti je zakotven ve smlouvě se zdravotnickým zařízením. Všichni zaměstnanci společnosti CGM jsou vázáni mlčenlivostí o údajích zjištěných v rámci výkonu svého povolání. Dodržování mlčenlivosti je součástí pracovních smluv zaměstnanců.

7. Bezpečnostní opatření / zabránění riziku

CGM přijímá veškerá technická a organizační bezpečnostní opatření za účelem zajištění ochrany Vašich osobních údajů jakož i osobních údajů Vašich pacientů před neoprávněným přístupem, úpravami, zveřejněním, ztrátou, zničením nebo jinými způsoby zneužití. Tato opatření zahrnují interní testování a kontroly našich procesů shromažďování dat, ukládání a zpracování. Dále zahrnují bezpečnostní opatření na ochranu informačních systémů, na kterých ukládáme smluvní údaje a data z technických operací, před neoprávněnými přístupy.

8. Technická a organizační opatření

K zajištění ochrany údajů provádí CGM pravidelný průzkum stavu vývoje v oblasti bezpečnostních technologií. To zahrnuje stanovení typických scénářů poškození, které pramení z odpovídajících bezpečnostních potřeb/úrovní bezpečnosti pro různé typy osobních údajů, které jsou slučovány do kategorií možných poškození, stejně jako provádění posouzení rizik.

Dále specializované penetrační testování, které je prováděno formou pravidelných testů, posuzování a vyhodnocování účinnosti těchto technických a organizačních bezpečnostních opatření, která zajišťují bezpečnost zpracování dat.

Následující pokyny upravují implementaci vhodných technických a organizačních opatření:

- **Zálohování dat (ordinace)**
Za účelem zamezení ztrátám dat jsou data pravidelně zálohována.
- **Ochrana soukromí**
CGM zajišťuje, aby byly ochrana údajů/soukromí a zásady ochrany údajů zohledněny v návrhu a vývoji procesů informačních systémů.

Cílem je vyhnout se nákladnému a časově náročnému dodatečnému programování, které by bylo potřeba provést, pokud by ochrana údajů a bezpečnostní požadavky měly být implementovány po zavedení informačního systému. Opatření jako deaktivace některých funkcí softwaru, ověření nebo šifrování, jsou zohledňovány na začátku procesu vývoje.

- **Ochrana soukromí**

CGM produkty jsou dodávány s továrním nastavením, které je optimalizováno na ochranu dat tím způsobem, že jsou zpracovávány pouze osobní údaje nezbytné k danému účelu.

- **Komunikace prostřednictvím e-mailu (lékařská praxe/CGM)**

V případě, že si přejete kontaktovat CGM prostřednictvím emailu, vezměte prosím na vědomí, že zásady ochrany předávaných informací nemohou být zaručeny, jelikož obsah emailových zpráv může být viděn třetími stranami. Doporučujeme používat poštovní komunikaci, pokud si přejete předávat důvěrné informace.

- **Vzdálená správa**

Zaměstnanci a subdodavatelé CGM mohou mít přístup k údajům o pacientovi nebo zákazníkovi a v určitých případech také k údajům o lékařské praxi. Tento přístup se řídí obecnými pravidly CGM.

- Vzdálený přístup k administraci je ve výchozím nastavení uzamčen a je udělován pouze zákazníkům.
- Hesla k přístupu do informačního systému zákazníka jsou vydávána pouze za účelem vzdálené správy systému.
- Kritické zásahy jsou zabezpečeny principem 4 očí s další kvalifikovanou osobou.
- Používáme nástroje vzdálené správy, které vyžadují aktivní potvrzení přístupu zákazníkem, což zákazníkovi umožňuje sledovat prováděné zásahy.
- Přístup formou vzdálené správy je zaznamenáván do CRM systému. Jsou zaznamenávány následující data: odpovědné osoby, datum a čas, délka trvání, cílový systém, nástroj vzdálené správy, stručný popis úkonů a v případě kritických zásahů také jméno (jména) další kvalifikované osoby v případě použití principu 4 očí.
- Zaznamenávání relací vzdálené správy je zakázáno.

9. Práva subjektu údajů

Osobní údaje provozovatele praxe a zaměstnanců lékařské praxe

Máte právo být informováni o uložených údajích o Vaší osobě, jakož i právo přístupu k těmto datům, máte právo provádět opravy, mazání, změny ve zpracování, přenášet data a máte právo vznášet námítky ke zpracování Vašich osobních údajů.

Máte právo kdykoliv odvolat svůj souhlas. Odvolání souhlasu je účinné do budoucna.

Máte právo podat stížnost příslušnému dozorovému orgánu, pokud se domníváte, že Vaše údaje byly zpracovávány nevhodným způsobem.

Zavazujeme se k odstranění všech smluvních údajů, přihlašovacích údajů a všech údajů z technických operací po ukončení Vaší smlouvy i bez Vaší předchozí žádosti.

Jsme však vázáni obchodními a daňovými zákony k dodržování zákonem stanovených lhůt pro uchování dat, které mohou přesahovat termín ukončení Vaší smlouvy. Data z technických operací jsou ukládána pouze po

Prohlášení o ochraně údajů v produktu MEDICUS

CompuGroup Medical Česká republika s.r.o.



dobu, která je z technického hlediska nezbytná, a jsou vymazány nejpozději po ukončení Vaší smlouvy.

Osobní údaje pacienta

Vaši pacienti mají právo být informováni o svých údajích, které ukládáte, jakož i právo obdržet a přenášet svá osobní data (přenositelnost dat) a právo provádět opravy, mazat, omezit zpracování a právo vznášet námitky proti zpracování svých osobních údajů.

Pokud však od pacienta obdržíte žádost o vymazání dat, jste povinni dodržet povinnou příslušnou lhůtu pro uchování údajů.

Vaši pacienti mají právo kdykoliv odvolat svůj souhlas, přičemž odvolání souhlasu má účinnost do budoucna.

Vaši pacienti mají právo podat stížnost příslušnému dozorovému orgánu, pokud se domnívají, že jejich údaje byly zpracovávány neodpovídajícím způsobem.

10. Vymahatelnost

Soulad s pravidly na ochranu dat, která jsou popsána v tomto dokumentu, je pravidelně a průběžně kontrolován společností CGM.

Pokud CGM ČR obdrží stížnost, bude společnost kontaktovat podavatele stížnosti za účelem vyřešení všech vyjádřených obav, které se týkají zpracování jeho osobních údajů.

CGM ČR se zavazuje poskytovat součinnost příslušnému správnímu úřadu i příslušnému dozorovému orgánu.

11. Dodatky k tomuto prohlášení o ochraně údajů

Vezměte prosím na vědomí, že toto prohlášení o ochraně údajů může podléhat změnám a dodatkům. V případě podstatných změn uveřejníme detailní oznámení o těchto změnách. Každá verze tohoto prohlášení o ochraně údajů je identifikována datem a číslem verze, které jsou uvedeny v zápatí dokumentu. Zároveň jsou všechny předchozí verze tohoto prohlášení archivovány a jsou k dispozici k nahlédnutí na žádost inspektora ochrany osobních údajů.

12. Odpovědná osoba CGM ČR

Generální ředitel Divize Ambulantní informační systémy

Vladimír Píkrýl

CompuGroup Medical Česká republika s.r.o.

Budova C, Coral Office Park, Bucharova 2657/12, 158 00 PRAHA 13

Pověřenec ochrany osobních údajů

V případě dotazů, týkajících se zpracování Vašich osobních údajů a vyřízení Vašich dotazů a stížností kontaktujte prosím Inspektora ochrany údajů.

Ing. Martin Roček

Telefon: (+420) 246 007 920

Email: GDPR.Officer.CZ@cgm.com

13. Příslušný dozorový orgán

Příslušným dozorovým orgánem pro CompuGroup Medical Česká republika s.r.o. je Úřad pro ochranu osobních údajů, sídlící na adrese Pplk. Sochora 27, 170 00 Praha 7.