

# OCHRANA OSOBNÍCH ÚDAJŮ (GDPR)

## Základní informace k GDPR

Účelem zveřejněných informací o ochraně osobních údajů je Vás přehledně a srozumitelně seznámit se způsobem nakládání s osobními údaji ve zdravotních zařízeních MEDICA SEVER s.r.o. (dále jen MEDICA) a to v souladu s legislativou Evropské unie a České republiky.

**Zákonná povinnost ochrany všech osobních údajů** spravovaných a zpracovávaných v MEDICA vyplývá z obecně platných zákonů:

- **Nařízení EU č. 2016/679** o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR).
- **Zákon č. 110/2019 Sb.**, o zpracování osobních údajů.

**Základní povinností MEDICA jako správce a zpracovatele osobních údajů je chránit osobní údaje tak, aby nedošlo k jejich úniku, ztrátě nebo zneužití.**

V MEDICA se jedná **především o osobní údaje pacientů, pacienty určených osob, zaměstnanců apod., a to jak v elektronické** (např. laboratorní informační systémy, personální systémy, datová úložiště atd.), **tak i papírové podobě** (např. kartotéky, zdravotní dokumentace, smlouvy, platební operace, kopie dokladů atd.).

**Tyto informace o ochraně osobních údajů jsou přednostně určeny pro pacienty, zaměstnance nebo jiné dotčené osoby ve vztahu k MEDICA.**

## Nařízení GDPR

### Co znamená GDPR

**Obecné nařízení o ochraně osobních údajů neboli GDPR (General Data Protection Regulation)** je dosud nejvíce uceleným souborem pravidel na ochranu dat na světě.

GDPR se týká každého, kdo s osobními údaji při svém podnikání či působení pracuje. Občané EU tak opět získají kontrolu nad svými osobními údaji.

Nařízení míří na firmy, instituce i jednotlivce, kteří zacházejí s osobními údaji – zaměstnanců, zákazníků, klientů či dodavatelů, a to napříč segmenty a odvětvími. Zasáhne i ty, kteří sledují či analyzují chování uživatelů na webu, při používání aplikací nebo chytrých technologií. Cílem GDPR je chránit digitální práva občanů EU.

GDPR platí v celé EU jednotně **od 25. května 2018**. V Česku tak nahrazuje současnou právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a vynutilo zrušení původního zákona č. 101/2000 Sb., o ochraně osobních údajů. Současný platný zákon č. 110/2019 Sb., o zpracování osobních údajů, již upřesňuje některé oblasti a dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů na vnitrostátní úrovni. U některých aspektů dokonce Obecné nařízení předpokládá vnitrostátní úpravu, mezi ně patří například: věk způsobilosti dítěte pro souhlas na 15 let, aspekty zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby.

To, že nová pravidla byla přijata formou evropského nařízení, znamená především jejich jednotnou platnost ve všech státech EU, aby je národní vlády a zákonodárci nemohli jakkoli ohýbat a přizpůsobovat místním zájmům nebo lobbistům.

Kompletní znění GDPR v českém překladu jako „**Obecné nařízení o ochraně osobních údajů**“ naleznete [zde](#).

### GDPR ve zdravotnictví

Osoby pracující ve zdravotnictví přicházejí každodenně do kontaktu s množstvím osobních údajů. Předmětem GDPR je co nejvíce ochránit fyzické osoby, jejichž osobní informace by měly být (zdravotnictví nevyjímaje) přísně chráněny před porušením jejich zabezpečení, tedy byť i náhodnému zničení, ztrátě, změně, nebo i neoprávněnému poskytnutí nebo zpřístupnění.

Ve zdravotnictví je třeba trvat na komplexnějším zpracovávání osobních údajů pacientů, členů jejich rodiny, zaměstnanců, ale především i osob zranitelných (děti) a osob, které souhlas se zpracováním osobních údajů nejsou schopny samy poskytnout.

Pro citlivé údaje zpracovávané ve zdravotnictví jsou **stanoveny přísnější podmínky** než pro obecné osobní údaje, jedná se o tyto typy údajů:

- **údaje o zdravotním stavu** (takové, které se týkají tělesného a duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu);
- **genetické údaje** (údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby);
- **biometrické údaje** (například zobrazení obličeje nebo daktyloskopické údaje);
- **další.**

Podmínkou zpracování zvláštních kategorií údajů je zejména to, že:

- **zpracování je nezbytné pro účely poskytování zdravotních služeb;**
- **zpracování je nezbytné z důvodu významného veřejného zájmu v oblasti veřejného zdraví;**
- **subjekt údajů (např. pacient) udělí výslovný souhlas s jejich zpracováním pro jeden nebo více stanovených účelů.**

#### **Souhlas se zpracováním osobních údajů ve zdravotnictví**

Pokud není zpracování prováděno na základě právního, smluvního vztahu nebo oprávněného zájmu je nezbytné pro subjekt údajů (např. pacient) poskytnout souhlas s jejich zpracováním, který je dle nařízení „svobodný, konkrétní, informovaný a jednoznačný projev vůle, ve kterém subjekt údajů prohlašuje, nebo jinak zjevně potvrzuje své svolení ke zpracování osobních údajů“.

## Informace o zpracování osobních údajů

V následujících členěných informacích jsou uvedeny základní informace o ochraně osobních údajů v MEDICA.

Pro koho je tato informace určena

V zájmu přehlednosti a srozumitelnosti připravila MEDICA informace o zpracování osobních údajů pro jednotlivé kategorie subjektů údajů zvláště. Tato **informace je přednostně určena pro pacienty, zaměstnance nebo jiné dotčené osoby ve vztahu k MEDICA.**

Přiměřeně jsou údaje obsažené v této informaci použitelné i ve vztahu ke zpracování osobních údajů dalších osob, jejichž osobní údaje můžeme zpracovávat v souvislosti s námi poskytovanými službami nebo produkty pro tyto subjekty:

- pacienti, jejich rodinné příslušníky i návštěvníky;
- osoby blízké nebo mající přístup k informacím o zdravotním stavu a zdravotnické dokumentaci;
- zmocněnci či zákonní zástupci našich nezletilých pacientů;
- zaměstnance, jak současné, tak i minulé a budoucí;
- opatrovníci právně nezpůsobilých osob;
- účastníci prováděných platebních transakcí;
- osoby vkládající hotovost na pokladně;
- jiné dotčené osoby, (např. externí dodavatelé, studenti, účastníci školení nebo vzdělávacích programů, uživatelé služeb, spolupracujících osob apod.);

Výše uvedený souhrn možných subjektů údajů budeme dále označovat také za „subjekty“.

Potenciálním subjektem je pro potřeby tohoto vysvětlení myšlena osoba, která s MEDICA jedná v souvislosti s poskytováním zdravotních služeb, uzavřením, trváním nebo ukončením pracovněprávního vztahu nebo uzavření smlouvy a v souvislosti s tím MEDICA zpracovává její osobní údaje.

### Účel zpracování osobních údajů

Mezi **hlavní účely zpracování osobních údajů patří tyto oblasti:**

- zdravotní služby a zdravotní péče;
- pracovněprávní vztah nebo žádosti o zařazení do výběrového řízení;
- dodání služby nebo zboží obsahující osobní údaje;
- smluvní vztahy obsahující osobní údaje;
- navazující služby a činnosti obsahující osobní údaje.

### Způsob zpracování osobních údajů

**Zpracování osobních údajů probíhá manuálně i automatizovaně v elektronických informačních systémech, a to v elektronické nebo listinné podobě, vždy při vysokém technickém, organizačním a personálním zabezpečení v souladu s legislativními požadavky.**

Jaké osobní údaje MEDICA shromažďuje a zpracovává

**Osobní údaje**, které má MEDICA povinnost zpracovávat i **bez souhlasu pacienta** (jako součást zdravotnické dokumentace), **zaměstnance nebo jiné dotčené osoby ve vztahu k MEDICA, zejména:**

- Identifikační údaje - osobní údaje sloužící k jednoznačné a nezaměnitelné identifikaci pacienta zaměstnance nebo jiné dotčené osoby ve vztahu k MEDICA (např. jméno, příjmení, titul, rodné číslo, bylo-li přiděleno, jinak datum narození, adresa trvalého pobytu aj.);
- Kontaktní údaje – osobní údaje umožňující kontakt s pacientem, zaměstnancem nebo jinou dotčenou osobou ve vztahu k MEDICA (zejména adresa bydliště, tel. číslo, e-mailová adresa), kontaktní informace osob oprávněných získávat informace o pacientovi aj.;
- Údaje o zdravotním stavu pacienta – údaje získané a zpracovávané v souvislosti s poskytováním zdravotních služeb;
- Osobní údaje zaměstnance v rozsahu přiměřeném účelu zaměstnání, vedených v osobním spise a mzdové složce zaměstnance;
- Případně další osobní údaje dotčené osoby ve vztahu k MEDICA dle povahy a typu vztahu k MEDICA.

**Osobní údaje**, které MEDICA zpracovává **se souhlasem pacienta, zaměstnance nebo jiné dotčené osoby ve vztahu k MEDICA**, jsou specifikovány vždy v konkrétním souhlasu se zpracováním osobních údajů, který subjekt osobních údajů může MEDICA udělit.

Doba uchovávání (zpracování) osobních údajů

Doba uchovávání (zpracování) osobních údajů se vztahuje k jednotlivým účelům zpracování a vyplývá ze zákonných povinností, smluvních vztahů, oprávněného zájmu nebo uděleného souhlasu a lze uvést některé časté případy:

- Zdravotní služby:
  - Ambulantní péče (tj. primární ambulantní péče, stacionární péče a specializovaná ambulantní péče mimo odbornosti psychiatrie, adiktologie, sexuologie) – 10 let od poslední návštěvy (objektivní promlčecí doba), popř. 15 let je-li to v zájmu pacienta s ohledem na vývoj jeho onemocnění (z důvodu ochrany práv a oprávněných zájmů MEDICA);
  - Specializovaná ambulantní péče – 50 let;
- Personální informace o zaměstnancích – 30 let;
- Osobní údaje žadatelů o práci – 3 měsíce po ukončení výběrového řízení;
- Osobní údaje, které zpracováváme na základě souhlasu subjektu pro stanovený účel, jsou zpracovávány po dobu, po kterou je souhlas platný, resp. do jeho odvolání.

V souladu se zásadou minimalizace dat je naším záměrem zpracovávat pouze ty osobní údaje, které nezbytně potřebujeme pro daný účel a jejich uchovávání je nastaveno tak, aby byly ponechány po nezbytně nutnou dobu k zajištění zájmů subjektu údajů nebo ochrany jeho práv či práv na ochranu zájmů MEDICA. Jakmile daná doba uplyne nebo pozbyly důvody uchování, jsou osobní údaje vymazány, resp. anonymizovány.

Komu dalšímu je umožněn přístup k mým osobním údajům

MEDICA Vaše osobní údaje sdílí s jinými správci osobních údajů pouze v případě, že na základě právního předpisu mají stanovenou povinnost či jsou k tomu oprávněni nebo pokud byste nám k tomu udělili souhlas.

Zákonná povinnost poskytování osobních údajů se vztahuje především na tyto subjekty:

- jiní poskytovatelé zdravotních služeb (např. jiné nemocnice, laboratoře, praktičtí lékaři pacienta apod.);
- ÚZIS, SÚKL, Národní zdravotní registry;
- státní instituce (Policii ČR, soudu, orgánům činným v trestním řízení, orgánu sociálního zabezpečení, Úřadu práce, obecnímu úřadu apod.);
- exekutor;
- zdravotní pojišťovny;
- zákonný zástupce.

Jednotlivé zákony upravují, za jakých podmínek mohou tyto osoby žádat poskytnutí údajů a v jakém rozsahu.

Pro sdílení osobních údajů se zpracovateli osobních údajů není Váš souhlas třeba. Subjekty, které se mají stát zpracovateli osobních údajů, jsou smluvně zavázány tyto údaje náležitě chránit. S každým subjektem, který by se v rámci své činnosti pro nás mohl stát zpracovatelem osobních údajů, které spravujeme, je uzavřena písemná smlouva o zpracování osobních údajů a tento zpracovatel je s osobními údaji oprávněn nakládat pouze v rozsahu nezbytně nutném pro splnění jeho úkolu, pro účely splnění jeho úkolu a po sjednanou dobu.

## Bezpečná komunikace a postupy

Níže jsou vysvětleny jednotlivé postupy nebo okolnosti ochrany osobních údajů doporučené MEDICA.

### Bezpečná komunikace

#### Proč je nezbytné chránit osobní údaje

V současné digitalizované době se zvyšují a zpřísňují požadavky nejen v rámci EU a ČR na ochranu osobních údajů. Tato povinnost se vztahuje i na ochranu zdravotnické dokumentace, osobních údajů pacientů a zaměstnanců MEDICA.

**Povinnosti ochrany všech osobních údajů spravovaných a zpracovávaných v MEDICA vyplývají z obecně platných zákonů a norem, které se vztahují na správce, tj. MEDICA, zejména:**

- **Nařízení EU č. 2016/679** o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR).
- **Zákon č. 110/2019 Sb.**, o zpracování osobních údajů.
- **Zákon č. 181/2014 Sb.**, o kybernetické bezpečnosti.

**Správce osobních údajů, tj. MEDICA, je povinen chránit osobní údaje tak, aby nedošlo k jejich zneužití.**

V MEDICA se jedná především o osobní údaje pacientů, pacienty určených osob, zaměstnanců, návštěvníků MEDICA apod., a to jak v elektronické podobě (např. personální systémy, datová úložiště, kamerové záznamy atd.) tak i papírové podobě (např. kartotéky, zdravotnická dokumentace, kopie dokladů atd.).

Osobním údajem jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, příjmení, rodné číslo, adresa, zdravotnická dokumentace / vyšetření nebo anamnéza, mobilní číslo, e-mail, atd.) nebo jakákoliv kombinace údajů, z kterých je osoba identifikovatelná (např. e-mail a jméno s příjmením).

#### Možnosti komunikace s lékaři

MEDICA, jako správce Vašich osobních údajů, které jsou obsaženy ve zdravotnických dokumentech, které můžete od našich lékařů obdržet (eRecept, výsledky vyšetření, lékařská zpráva apod.) dbá na ochranu Vašeho soukromí.

**Z tohoto důvodu nabízíme tyto formy komunikace s lékařem:**

- Osobně
- Doporučeným dopisem
- **E-mailem nebo telefonem v případě akceptace „Souhlasu se zasíláním osobních údajů na e-mail telefon“**
- E-mailem s vlastním kvalifikovaným elektronickým podpisem (vydává kvalifikovaný poskytovatel certifikačních služeb – [přehled](#))
- Registrací do [Centrálního úložiště eReceptů](#) přímo na SÚKLu – pouze pro eRecepty!

**Možnost souhlasu subjektu se zasíláním osobních údajů e-mailem, telefonem**

V případech, kdy subjekt požaduje zaslání informací o vyšetření, diagnóze, eReceptu, medikace a jiné osobní informace, na e-mail nebo telefon, je **nezbytně nutné nejdříve pochopit a akceptovat zaslání upozornění na rizika vyplývající ze zaslání osobních údajů běžným e-mailem nebo telefonem ze strany subjektu**. Běžný e-mail je nezabezpečenou formou komunikace, tj. bez využití např. šifrování obsahu, kde nelze garantovat mimo jiné to, že jeho obsah nebude po odeslání přečten či upraven neautorizovanou osobou.

#### **Jak v těchto případech postupovat:**

1. Zašlete požadavek na zaslání informací o vyšetření, diagnóze, eReceptu, medikace a jiné osobní informace na e-mail nebo telefon zaměstnance MEDICA.
2. K požadavku přiložíte podepsaný „Souhlas se zasíláním osobních údajů na email\_telefon“, kde jste upozorněni na rizika se zasíláním osobních informací běžným e-mailem nebo telefonem a svým podpisem uvedené rizika akceptujete. Požadované údaje Vám následně budou zaslány na e-mailovou adresu nebo telefonní číslo uvedené v souhlasu.
3. Neudělíte-li tento souhlas, vyžádané dokumenty Vám budou poskytnuty jinou cestou, např. v tištěné podobě.

#### **Udělení souhlasu subjektu**

V případech, kdy je nezbytný souhlas se zpracováním osobních údajů pacienta, zaměstnance nebo případně další osoby, **bude souhlas se zpracováním osobních údajů splňovat následující podmínky**, tj. být:

- **svobodně udělený** (pokud není udělen, nebude znamenat znevýhodnění);
- **informovovat o účelu a rozsahu souhlasu;**
- **srozumitelně a jednoznačně formulován;**
- **zřetelně oddělen od jiného textu;**
- **kdykoliv odvolatelný stejně snadno, jako byl dán.**

#### **Zadání požadavku zaměstnance nebo pacienta dle práv definovaných v GDPR**

Pacient nebo zaměstnanec (stejně jako další osoby) má nárok dle práv definovaných v GDPR:

- **na žádost o informace o zpracovávaných osobních údajích;**
- **na žádost o výmaz osobních údajů;**
- **na vznesení námítky proti zpracování svých osobních údajů;**
- **požádat o přenositelnost zpracovávaných osobních údajů;**
- a další

a zadá svůj požadavek:

- **Pacient, bývalý zaměstnanec, stejně jako další osoby:**
  - zašle poštou: písemně s úředně ověřeným podpisem žadatele, přičemž tato žádost musí být zaslána na adresu MEDICA;
  - osobním doručením žádosti na adresu Domky 109,460 10, Liberec, následně v procesu vyřízení žádosti bude ověřena totožnost žadatele;
  - zašle e-mailem na adresu [info@medicasro.cz](mailto:info@medicasro.cz), za předpokladu, že žadatel e-mail podepíše vlastním kvalifikovaným elektronickým podpisem;
  - zašle datovou schránkou, za předpokladu, že žadatel se shoduje s odesílatelem datové zprávy.
- **Zaměstnanec (v pracovním poměru):**
  - zašle z pracovního e-mailu (.....@medicasro.cz) na adresu [info@medicasro.cz](mailto:info@medicasro.cz).



## Nahlášení podezření nebo zjištění úniku osobních údajů

V případě **podezření nebo zjištění úniku osobních údajů** či **jejich zneužití**, mám možnost tuto skutečnost **nahlásit pověřenci na ochranu osobních údajů** MEDICA (kontakt uveden níže).

## Kam se obrátit při potřebě vyjasnění ochrany osobních údajů

Při potřebě vyjasnění ochrany osobních údajů se obraťte na pověřence na ochranu osobních údajů MEDICA, který zajišťuje tyto oblasti:

- nezávislou kontrolní a poradenskou funkci ve vztahu k osobním údajům;
- sledování a vyhodnocení stavu souladu MEDICA s požadavky GDPR;
- komunikaci se subjekty osobních údajů (např. pacienti, zaměstnanci) při využití svých práv dle nařízení GDPR (např. právo na informace, výmaz, námitku, přenositelnost);
- komunikaci s ÚOOÚ a hlásí případné případy narušení ochrany osobních údajů.

Kontaktní údaje na pověřence na ochranu osobních údajů MEDICA jsou uvedeny níže.

## Pověřenec pro ochranu osobních údajů MEDICA

kontaktní e-mail: [info@medicasro.cz](mailto:info@medicasro.cz)