Koncept výmazu osobních údajů v produktu MEDICUS

CompuGroup Medical Česká republika s.r.o.

Obsah

1 Výklad pojmů

Výklad pojmů používaných dále v celém dokumentu "GDPR - koncept výmazu osobních údajů".

1.1 Osobní údaje (OÚ)

Osobní údaje jsou jakékoli informace o identifikovaném nebo identifikovatelném subjektu údajů. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Poznámka 1: Mezi OÚ patří i údaje, které nejsou zpracovávány (a uchovány) elektronicky - tedy například papírová dokumentace

1.2 Správce OÚ

Správce osobních údajů je podle GDPR každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí za jím stanoveným účelem jejich shromažďování, zpracování a uchování. Správce primárně odpovídá za zpracování osobních údajů.

1.3 Zpracovatel osobních údajů

Poskytovatel služeb, který zpracovává osobní údaje jménem správce osobních údajů a výhradně v souladu se smluvními ustanoveními.

1.4 Anonymizace

Nevratný proces, kterým se osobní údaje pacienta změní tak, že pacienti již nemohou být přímo nebo nepřímo identifikovány.

Poznámka 1: Za účelem anonymizace jsou jednotlivé osobní údaje pacienta, které umožňují jeho identifikaci například vymazány nebo přepsány. Zbývající údaje (u kterých bylo anonymizací vyloučeno jakékoliv spojení s původní osobou) již nepodléhají předpisům o ochraně osobních údajů, a proto již nepodléhají ani požadavkům na vymazání. Anonymizace je často obtížné dosáhnout.

Poznámka 2: Proces anonymizace je mimo jiné založen i na standardu ISO / IEC 29100: 2011

1.5 Minimální doba uchování dat

Minimální doba uchování dat je doba, po kterou musí být údaje pacienta určité kategorie uchována a dostupná pro další použití. Tato doba je obvykle definována odpovídajícími zákony a vyhláškami.

Poznámka 1: minimální doby uchování dat jsou zdrojem pro výpočet doby, po kterou se musí uchovávat data pacienta, popřípadě doby, po které je nutné zařadit data pacienta do procesu skartace.

Poznámka 2: většina "minimálních dob uchování dat" pro jednotlivé kategorie zdravotnické dokumentace je definována ve vyhlášce 98/2012 " Vyhláška o zdravotnické dokumentaci".

1.6 Kategorie osobních údajů

Skupina údajů pacienta, které jsou zpracovávány pro stejný účel.

1.7 Datové objekty

Objekty, které obsahují data. Například soubory, dokumenty, sady dat či atributů. Jinými slovy například jména, adresy, telefonní čísla, e-mailové adresy.

Poznámka 1: Datové objekty mohou být v rámci určité kategorie údajů kombinovány s jinými datovými objekty. Jednotlivé datové objekty mohou mít různou složitost - tzn. od různých souborů dat po datové objekty typu "atribut".

1.8 Výmaz dat

Proces, pomocí kterého jsou osobní údaje změněny nevratným způsobem tak, že poté buď:

- již neexistují
- nebo jsou nerozpoznatelné a nemohou být dále používány nebo rekonstruovány.

Poznámka 1: Obvykle bývá v souvislosti s osobními údaji požadováno "bezpečné smazání" dat. Bezpečné smazání znamená, že úsilí spojené s rekonstrukcí smazaných dat je tak velké, že je to nemožné nebo je to možné pouze s velmi významným (neúměrným) úsilím (náročnost na osoby, nástroje a čas).

Poznámka 2: Pokud to umožňují příslušná pravidla ochrany údajů, mohou být osobní údaje anonymizovány namísto jejich odstranění.

1.9 Koncept výmazu osobních údajů

Soubor ustanovení a pravidel, která pomohou správci údajů zajistit, aby veškeré soubory osobních údajů, které zpracovává (uchovává) byly smazány v termínech a způsobem, které jsou v souladu s platnou legislativou a nařízeními.

2 Základ konceptu výmazu osobních údajů

2.1 Obecné informace

Tento dokument popisuje možnosti a pravidla mazání osobních údajů v ambulantních systémech CGM ČR. Příslušné právní předpisy o ochraně osobních údajů (GDPR) vyžadují od správce OÚ (našeho zákazníka jako uživatele ambulantního systému CGM ČR), aby umožnil na žádost subjektu údajů vymazání osobních údajů, tedy i osobních údajů pacientů uložených v našich ambulantních systémech.

V tomto konceptu výmazu OÚ specifikujeme nebo doporučujeme, jak by měl lékař, správce OÚ, k mazání OÚ přistupovat, aby naplnil povinnosti dané GDPR, ale také jinými právními předpisy, kterými se ordinace musí řídit. V následujícím dokumentu specifikujeme zejména:

- kategorie osobních údajů a jakými právními předpisy je odstranění těchto dat upraveno;
- jak je mazání dat prováděno a dokumentováno;
- kdo je zodpovědný za implementaci procesu výmazu OÚ (revize a aktualizaci činností vyplývajících z konceptu výmazu)

V této části jsou definovány jednotlivé bloky, ze kterých se koncept mazání OÚ skládá, v dalších částech dokumentu jsou pak tyto bloky podrobněji popsány.

Koncept mazání OÚ je určen pro implementaci vybraných povinností odpovědné osoby správce OÚ v oblasti ochrany údajů. Dokument lze proto chápat jako součást dokumentace ochrany údajů v ordinaci.

2.2 Aplikace nařízení GDPR pro ochranu údajů

Instrukce pro mazání osobních údajů vyplývají z nařízení GDPR o ochraně osobních údajů a případně také z dalších právních předpisů.

V tomto dokumentu se výrazem "relevantní" rozumí všechna ustanovení, na jejichž základě jsou všechny soubory osobních údajů zaznamenávány a zpracovávány a které by měly nebo musí být (na žádost subjektu údajů nebo i bez ní) vymazány. Při plnění povinnosti výmazu osobních údajů jsou kromě příslušných předpisů o ochraně údajů (GDPR) relevantní i další právní předpisy nebo dokumenty (např. smlouvy). Úkolem správce OÚ je samozřejmě dodržování všech zákonných ustanovení, který se vztahují na OÚ zpracovávané v ordinaci lékaře.

2.2.1 Výmaz OÚ ve vztahu k (smluvním) zpracovatelům OÚ

V rámci ochrany dat je nutné, aby každý správce OÚ měl s případným zpracovatelem OÚ uzavřenou tzv. "zpracovatelskou smlouvu", tedy smlouvu týkající se zpracování osobních údajů. Správce OÚ pomocí "zpracovatelské smlouvy" musí zajistit, aby smluvní zpracovatel zpracovával osobní údaje pouze v rozsahu a účelu definovaném správcem. Správce osobních údajů je zodpovědný za stanovení a předpisů v oblasti ochrany osobních údajů včetně předpisů v oblasti výmazu OÚ a dodržování těchto předpisů musí být zajištěno nejen u samotného správce, ale i u všech případných smluvních zpracovatelů OÚ.

Pokud chce správce osobních údajů přizpůsobit své předpisy v oblasti ochrany, či výmazu OÚ přání smluvního zpracovatele, může tak učinit pouze tehdy, pokud jsou příslušná ustanovení pro správce přípustná.

2.3 Co znamená "výmaz OÚ"?

Datové objekty, které se týkají určité osoby, se považují za vymazané, pokud již neexistují nebo je nelze přiřadit určité osobě a nemohou být již použity ve vztahu k této osobě. Vymazání je dosaženo například fyzickým přepsáním datových objektů. Datové objekty mohou být také odstraněny vhodným zničením datových nosičů, na kterých jsou uloženy. Které postupy jsou použity pro odstranění nebo zničení závisí na citlivosti dat, nosičích dat a příslušných předpisech o ochraně dat. Výběrem konkrétních postupů se tento obecný pokyn nezabývá.

Datové objekty mohou být namísto jejich odstranění také anonymizovány. Pokud nelze k datovým objektům určit žádnou konkrétní osobu, již se na tyto datové objekty nevztahují předpisy o ochraně a odstranění osobních údajů. Často je však velmi obtížné správně anonymizovat data, aby na základě sady dat nebylo možné zpětně identifikovat osobu. Proto se doporučuje upřednostnit vymazání dat.

POZNÁMKA: přestože anonymizované údaje již nepodléhají postupům pro mazání osobních údajů dle nařízení o ochraně dat, i nadále se jedná o důvěrná data odpovědného organizace - správce dat.

V následujícím textu bude nadále používán pouze výraz "výmaz" (popřípadě "mazání"), který bude zahrnovat všechny alternativy implementace mazání OÚ, tedy i "zničení datových nosičů" či "anonymizaci dat".

2.4 Nařízení mazání osobních údajů pro každý typ / kategorii OÚ

2.4.1 Kategorie OÚ

Kategorie dat ukládaných a zpracovávaných v ambulantním (popřípadě zubařském) informačním systému

- **Zdravotní dokumentace pacientů (včetně osobních údajů pacientů)**
  Zdravotnická dokumentace (dále jen "ZD") je definována oborovou legislativou, zejména Zákonem o zdravotních službách č. 372/2011 Sb. ve znění pozdějších předpisů (dále jen "ZZS"). Způsoby nakládání, vyřazovací znaky a lhůty pro uchovávání jsou řízeny Vyhláškou o zdravotnické dokumentaci č. 98/2012 Sb, přičemž se s ZD pracuje vždy pro daného pacienta a organizační jednotku zdravotnického zařízení jako s celkem.
- **Objednávky návštěv neznámých osob (objednávky - termíny návštěv, žádanky na vyšetření)**
  Systém ukládá data o objednávkách návštěv popřípadě žádankách o vyšetření osob, kteří nejsou dosud v systému vedeny.
  Pokud se tyto osoby dostavily k návštěvě (vyšetření), pak se odpovídající záznamy stávají součástí zdravotnické dokumentace. V opačném případě se nejedná o součást ZD.
- **Daňové doklady a platební informace**
  Uložení dokladů souvisejících s účtováním provedených služeb pacientovi nebo jinému plátci je upraveno Zákonem o účetnictví č. 353/2001 a Zákonem o DPH č. 235/2004.
  Zároveň jsou uchovávány platební informace o pojištění pacienta u zdravotní pojišťovny za účelem vyúčtování zdravotní péče, popřípadě informace o samoplátcích.
- **Auditní stopa**
  Data poskytují nezbytné informace pro splnění zákonných povinností daných ZZS, povinností stanovených v rámci Obecného nařízení o ochraně osobních údajů č. 2016/679 (dále jen "GDPR") a pro zajištění potřebné úrovně poskytování služeb dodavatelem CompuGroup Medical Česká republika s.r.o.
  S odkazem na Stanovisko č. 3/2015 vydané Úřadem pro ochranu osobních údajů je lhůta pro uchování stanovena na 1 rok.
- **Nastavení systému**
  Pro řádnou funkci systému jsou uchovávána související technická a provozní nastavení.

2.4.2 Nařízení o výmazu OÚ

Osobní údaje by neměly být odstraňovány v jednotlivých případech, ale měly by být mazány důsledně v souladu s patřičnými předpisy. Pro každý kategorii a účel zpracování OÚ jsou dána pravidla jejich výmazu, která vyhovují jak předpisům o ochraně dat (GDPR), tak dalším odpovídající předpisům (legislativním nebo vnitřním předpisům ordinace).

Každé pravidlo o výmazu OÚ musí obsahovat jak časový limit pro odstranění OÚ tak i informaci, od jaké události se tento časový limit počítá (dle kategorie dat, popřípadě i dle dalších parametrů nemusí být touto událostí pouze datum záznamu OÚ, ale například datum narození či úmrtí pacienta). Dále budou v tomto dokumentu definována pravidla pro výmaz jednotlivých kategorií OÚ, pro jejichž zpracování je určen náš ambulantní systém.

Právní předpisy o ochraně údajů obvykle vyžadují, aby byly osobní údaje vymazány, pokud již nejsou potřebné nebo pokud vypršela zákonná či jiná lhůta pro zpracování. V souladu s tím by měly být osobní údaje vymazány co nejdříve. Přesné vysvětlení pojmu "co nejdříve" bude uvedeno u každé kategorie OÚ.

2.5 Minimální doby uchování dat (a následný výmaz) jednotlivých kategorií OÚ

2.5.1 Standardní proces mazání OÚ

Datové objekty by měly být vymazány **ve všech systémech odpovědné osoby (správce)** po uplynutí lhůty pro uchování daného typu OÚ. To zahrnuje samozřejmě výmaz dat i u smluvních zpracovatelů OÚ daného správce.

V ambulantním systému jsou ukládány také data, u kterých není žádným právním předpisem přesně stanovena minimální doba pro jejich uchování (zpracování). Jde například o objednávky pacientů (zejména těch, kteří se nedostaví k vyšetření) nebo například o auditní stopa, ve které jsou uchovány informace o všech činnostech uživatelů v ambulantním systému a zejména pak o přístupech k OÚ pacientů. Úkolem správce osobních údajů (zákazníka, majitele ordinace a podobně) je, aby posoudil s ohledem na zájmy vlastní organizace, jak dlouho bude taková data uchovávat a jaký si stanoví limit pro výmaz těchto typů dat. Po uplynutí takto stanované doby uchování dat může a musí být odstranění provedeno.

2.5.2 Péče o data, která nejsou součástí produkčního prostředí ambulantního systému - archivní a záložní kopie dat

Pro tento koncept výmazu OÚ je nutné jasně rozlišovat mezi **archivy** a **záložními kopiemi**.

Archivy slouží k dlouhodobému ukládání dat. Data se ukládají do archivu, pokud se nepředpokládá jejich aktivní využití, avšak existují povinnosti uchování těchto dat. Archiv může obsahovat různé kategorie dat s odlišnými minimálními dobami uchování. Pro data uložená v archivu musí platit stejná pravidla a minimální doby uchování (dle kategorií a účelu zpracování) jako pro ostatní OÚ ordinace zpracovávané například v databázi ambulantního systému.

Záložní kopie dat (databází a jiných datových souborů) jsou vytvořeny tak, aby umožňovaly obnovu systému a všech jeho dat po poruše (havárii) a nemohou tedy být nijak modifikovány. Vymazání dat v rámci záložních kopií dat je prakticky velmi obtížné a je v přímém rozporu s vlastním účelem zálohování. Požadovaná doba uchovávání jednotlivých záložních kopií, tak aby záloha správně plnila svůj účel (obnovu systému), je krátká. Z provozního pohledu je naprosto dostateční, pokud je doba uchování zálohy 1 až 2 měsíce. **Každopádně doporučujeme, aby doba uchování záložní kopie nepřesáhla 12 měsíců.** Za takových okolností a pak zálohy splňují ustanovení o mazání dat.

Důrazně doporučujeme jasné rozlišení a oddělení záložních kopií od archivu. **Osobní údaje v archivech podléhají pravidlům pro mazání OÚ** a OÚ v archivu by tedy měly být v souladu s těmito pravidly mazány!

2.5.3 Výmaz dat ve speciálních situacích

Mimo standardní procesy výmazu OÚ definované v interních směrnicích organizace může být požadován výmaz OÚ ve specifických situacích, jako jsou například:

- výmaz neoprávněně zaznamenaných OÚ;
- výmaz OÚ na základě legitimní žádosti subjektu údajů (například pacienta);
- výmaz OÚ po odinstalaci (přeinstalaci na nový HW) systému z počítače organizace
- výmaz OÚ v případě převodu nebo rozdělení společnosti

Pro případ těchto a podobných specifických situací je třeba v rámci organizace také definovat opatření pro výmaz - zejména je nutné upřesnit kdo je zodpovědný za výmaz OÚ v organizaci a kdo tudíž musí zabezpečit proces výmazu i v těchto nestandardních situacích. Pro tyto specifické situace se procesy výmazu obvykle nedefinují.

3 Příloha A: Doby uchování dokumentace

V ambulantním systému jsou ukládány data různých kategorií.

Zdravotnická dokumentace

Mazání zdravotnické dokumentace se v systému vyhodnocuje dle vyhlášky 98/2012 s frekvencí minimálně jednou za pět let, může se ale i častěji (u velkých zařízení to má význam) a pak se provádí s frekvencí nejvýše 1x za rok

Na základě data poslední návštěvy v ordinaci nebo posledního ošetření, dle typu poskytované péče a dle dalších údajů se stanoví lhůta, ve které má dojít ke skartaci. Přesnější informace dle vyhlášky 98/2012 jsou uvedeny dále v tabulce.

Skartace zdravotnické dokumentace pacienta za pracoviště probíhá vcelku - tedy musí se vyhodnotit minimální doby uchování veškeré zdravotnické dokumentace pacienta a skartace celé dokumentace pacienta se provádí až uplyne minimální doba uchování veškeré dokumentace pacienta.

Při skartaci se po uplynutí předepsané lhůty pro uchování postupuje dle přiřazeného vyřazovacího znaku. Systém oprávněnému uživateli umožní zdravotnickou dokumentaci **se znakem S** smazat tak, aby byla znemožněna rekonstrukce a identifikace jejího obsahu. O smazání se vytvoří protokol.

Systém oprávněnému uživateli umožní u zdravotnické dokumentace **se znakem V** rozhodnout, zda lhůtu prodloužit, nebo zda zdravotnickou dokumentaci zařadit k vyřazení.

Objednávky návštěv neznámých osob

Záznamy o objednávkách návštěv, popřípadě žádankách o vyšetření osob, které nejsou dosud v systému vedeny a nedostavily se k návštěvě (vyšetření), jsou po roce od poslední operace se záznamem automaticky smazány.

Daňové doklady a platební informace

Po uplynutí zákonné lhůty 10 let od konce účetního období, ve kterém vznikly, jsou odpovídající záznamy smazány.

Auditní stopa

S odkazem na Stanovisko č. 3/2015 vydané Úřadem pro ochranu osobních údajů je doporučená lhůta pro uchování dat v auditní stopě 1 rok.

Záznamy se automaticky po stanovené lhůtě 1 rok smažou.

Nastavení systému

Data o nastavení systému jsou v systému trvale uložena a přepisují se nebo mažou průběžně tak, jak je to potřebné k řádnému běhu systému.

Minimální doby uchování zdravotnické dokumentace pacienta dle vyhlášky 98/2012:
(jsou zde jmenovány pouze typy dokumentace, které jsou uchovávány v AIS CGM ČR)

Typ dokumentace (typ dle vyhlášky 98/2012 - příloha 3)	**Minimální doba uchování**	**Vyřazovací znak**
1. a) Dokumentace zdravotní péče poskytované registrujícím praktickým lékařem (001)	10 let od úmrtí nebo 10 let od registrace k jinému lékaři	S
1. b) Dokumentace zdravotní péče poskytované registrujícím praktickým lékařem pro děti a dorost (002)	10 let od úmrtí nebo 10 let od registrace k jinému lékaři nebo 10 let od dovršení 19-ti let pacienta	S
1. c) Dokumentace zdravotní péče poskytované registrujícím lékařem v oboru zubní lékařství nebo v oboru gynekologie a porodnictví (014, 603)	5 let od posledního poskytnutí zdravotních služeb	S
2. Dokumentace ostatní ambulantní péče	5 let od posledního poskytnutí zdravotních služeb	V
3.a) Dokumentace dispenzární péče	10 let od úmrtí nebo 10 let od vyřazení pacienta z dispenzární péče	V
3.b) Dokumentace dispenzární péče - dialyzovaný pacient	10 let od úmrtí	V
3.c) Dokumentace dispenzární péče - nosič infekčního onemocnění	10 let od úmrtí	V
4. Dokumentace léčby duševních poruch a poruch chování (včetně ochranné léčby)	10 let od úmrtí	S
5. a) Dokumentace lůžkové péče	10 let od úmrtí nebo 40 let od poslední hospitalizace	S
5. b) Dokumentace lůžkové péče - následná nebo dlouhodobá péče	10 let od úmrtí nebo 20 let od poslední hospitalizace	S
6. Dokumentace jednodenní péče	10 let od úmrtí nebo 10 let od posledního poskytnutí jednodenní péče POZN: - jednodenní obory mají v odbornosti uprostřed "J" - **jsou to**	S

	odbornosti 5J1, 6J1, 6J3, 6J6, 7J1, 7J6 (celkem 104 IČP v ČR dle číselníku IČP od VZP)	
7. Dokumentace lázeňské léčebně rehabilitační péče	5 let od ukončení péče	
11.a) zobrazovací metody - obrazový záznam	10 let od ukončení posledního vyšetření pacienta	V
11.b) zobrazovací metody - informace o průběhu a výsledku vyšetření pacienta zobrazovací metodou	5 let od ukončení posledního vyšetření pacienta TOTO DĚLAT (podobně jako bod 2. ale jiný vyřazovací znak)	S
11.c) zobrazovací metody -obrazový záznam (u poskytovatele, který záznam nepořídil, ale obdržel)	1 rok od obdržení záznamu	S
11.d) zobrazovací metody - obrazový záznam, který je pořízen v souvislosti s onemocněním pacienta, pro které je pacient dispenzarizován (nebo obdobně sledován)	30 let od ukončení posledního vyšetření pacienta nebo 10 let od úmrtí	V
11.e) zobrazovací metody - veličiny a parametry umožňující stanovení dávky z lékařského ozáření	10 let od provedení lékařského ozáření	S
13. Lékařské předpisy s modrým pruhem (stanoveno jiným právním předpisem - zákon č. 167/1998 Sb. §33)	5 let	S
15.a) Žádanka o vyšetření (u poskytovatele vyšetření)	2 roky od vyšetření	S
15.b) Žádanka o vyšetření - karta pro novorozenecký screening	5 let od vyšetření	S
15.c) Žádanka o vyšetření - zobrazovací metody využívající ionizující záření	10 let od vyšetření	S
17. Záznam o podání léčivého přípravku pro moderní terapii, o dárcovství tkání a	30 let od podání léčivého přípravku pro moderní terapii, od odběru	V

buněk pro použití u člověka a o použití tkání nebo buněk u člověka	tkání a buněk pro použití u člověka a od použití tkání nebo buněk u člověka nebo 10 let od úmrtí pacienta	
19. Zdravotnická dokumentace o osobách ve výkonu vazby, trestu odnětí svobody nebo zabezpečovací detence vedená Vězeňskou službou České republiky	10 let od úmrtí	S