

KRITICKÉ
MOMENTY
ZPRACOVÁNÍ
OSOBNÍCH ÚDAJŮ
DLE GDPR PŘI
POSKYTOVÁNÍ
ZDRAVOTNÍ PÉČE



Efektivní právní služby

Obsah

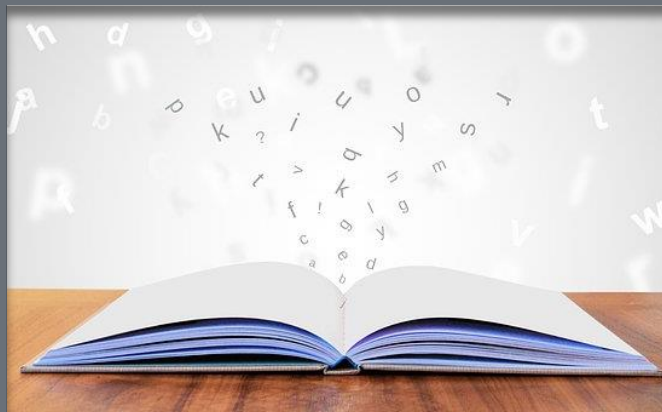
I. Úvod do problematiky ochrany osobních údajů

1. Legislativní rámec ochrany osobních údajů
2. Dozor v oblasti ochrany osobních údajů
3. Základní zásady zpracování osobních údajů
4. Vybrané základní pojmy dle GDPR
5. Základní zásady zpracování osobních údajů

II. Specifika zpracování osobních údajů při poskytování zdravotní péče

1. Zpracování osobních údajů při poskytování zdravotní péče
2. Vedení zdravotnické dokumentace dle GDPR
3. Kybernetická bezpečnost ve zdravotnictví a GDPR
4. Závěr

Úvod do problematiky ochrany osobních údajů



Legislativní rámec ochrany osobních údajů

- Ochrana soukromí fyzických osob v souvislosti se zpracováním osobních údajů je základním právem zakotveným na národní i Evropské úrovni.
- Ustanovení čl. 10 odst. 3 Listiny základních práv a svobod, jakož i čl. 8 odst. 1 Listiny základních práv Evropské unie přiznávají každé fyzické osobě právo na ochranu osobních údajů, které se jí týkají.
- **Nařízení (EU)2016/679** o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR) je přímo účinný právní předpis **od 25. května 2018**
- Návrh (tzv. adaptačního) **zákona o zpracování osobních údajů**, jež nahradí zákon č. 101/2000 Sb. o ochraně osobních údajů, je v legislativním procesu. Jedná se o sněmovní tisk č. [138](#) (ZZOÚ) a sněmovní tisk č. [139](#) (doprovodný zákon)

Dozor v oblasti ochrany osobních údajů

- Nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí WP29 (Pracovní skupina dle čl. 29) byl nahrazen **Evropským sborem pro ochranu osobních údajů** složený z jednotlivých vedoucích dozorových úřadů členských států a evropského inspektora ochrany údajů, či jejich zástupců.
- Hlavním úkolem sboru je nezávisle přispívat k jednotnému uplatňování GDPR v celé EU, k čemuž jí GDPR přiznává řadu pravomocí rozhodovacího, kontrolního i poradního charakteru
- Pro některé případy přeshraničního zpracování zakotvuje GDPR s cílem efektivnější regulace tzv. vedoucí dozorový úřad
- **Úřad pro ochranu osobních údajů ČR** musí stejně jako ostatní dozorové úřady při své činnosti dodržovat mechanismus jednotnosti za účelem jednotného uplatňování GDPR v celé EU
- Každá FO i PO má i nadále právo na účinnou soudní ochranu u příslušného **vnitrostátního soudu** proti rozhodnutím dozorového úřadu, která vůči ní zakládají právní účinky.

Vybrané základní pojmy dle GDPR

- GDPR přebírá řadu klíčových definic a navazuje ve sledovaných cílech a obsahových zásadách zpracování dat na směrnici 95/46/ES
- **osobními údaji** se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě, která je označována jako subjekt údajů; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat;
- **zpracováním** se rozumí jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů;
- **správce** se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
- **zpracovatelem** se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje za správce;

Základní zásady zpracování osobních údajů

- Za nejvýznamnější systémové změny, které GDPR přineslo lze označit komplexní promítnutí principů:
 - **Záměrné a standardní ochrany OÚ (Privacy by design)**
 - **Přístup založený na riziku (Risk based approach)**
- Zákonné zpracování osobních údajů musí být vždy založeno na některém z právních titulů, který stanoví GDPR a který musí odpovídat předem stanovenému účelu zpracování údajů
- Jednotlivé právní tituly rozlišují případy zpracování osobních údajů a tzv. zvláštních kategorií osobních údajů a také zpracování osobních údajů, které vyžaduje nebo nevyžaduje souhlas subjektu údajů či jeho zástupce
- GDPR klade velký důraz na transparentnost zpracování údajů
- Další klíčové zásady zpracování osobních údajů dle GDPR jsou minimalizace, přesnost, omezení (doby) uložení, integrita a důvěrnost osobních údajů a také zásada odpovědnosti správce za zajištění a prokázání souladu zpracování s GDPR

Specifika zpracování osobních údajů při poskytování zdravotní péče



Zpracování osobních údajů při poskytování zdravotní péče

- Důležitým předpokladem souladu s GDPR je pro lékaře schopnost identifikovat a zdokumentovat:
 - jaké osobní údaje zpracovává;
 - na základě jakého právního titulu je zpracovává;
 - kde je shromažďuje;
 - kdo je oprávněn k nim a jakým způsobem přistupovat;
 - jak je zajištěna jejich ochrana;
 - jak jsou případně likvidovány
- V širší souvislosti s poskytováním zdravotní péče ze strany lékaře je možné identifikovat hned několik činností, při kterých nutně dochází ke zpracování osobních údajů
- Kromě stěžejní a nevyhnutelné činnosti spočívající ve vedení zdravotní dokumentace se může jednat o evidenci vedenou pro vyúčtování tzv. nehrazených (smluvních) zdravotních služeb, při plnění farmakovigilančních povinností, vedení personální a mzdové agendy, výzkumnou činnost a klinická hodnocení, provoz kamerového systému či jiný monitoring pracoviště atd.

Vedení zdravotnické dokumentace dle GDPR

- Stěžejní zpracovatelskou činností kontrolovanou lékařem v postavení správce údajů dotčených osob při poskytování zdravotní péče je **vedení zdravotnické dokumentace**
- Jedná se o zpracování osobních údajů, které je nezbytné pro **splnění právní povinnosti** správce (čl. 6 odst. 1 písm. c)
- Zpracování zvláštních kategorií osobních údajů ve zdravotní dokumentaci, tj. především údajů **o zdravotním stavu** pacienta GDPR výslovně připouští (čl. 9 odst. 2 písm. h)
- Zvláštní kategorie osobních údajů mohou být zpracovávány pro účely uvedené v odst. 2 písm. h) pouze pracovníkem vázaným služebním tajemstvím nebo jinou osobou vázanou povinností mlčenlivosti (čl. 9 odst. 3 GDPR)
- Členské státy mohou dle čl. 9 odst. 4 GDPR zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či **údajů o zdravotním stavu**

Vedení zdravotnické dokumentace dle GDPR

„Mezi osobní údaje o zdravotním stavu by měly být zahrnuty veškeré údaje související se zdravotním stavem subjektu údajů, které vypovídají o minulém, současném či budoucím tělesném nebo duševním zdraví subjektu údajů. To zahrnuje informace o dané fyzické osobě shromážděné v průběhu registrace pro účely zdravotní péče a jejího poskytování dotčené fyzické osobě podle směrnice Evropského parlamentu a Rady 2011/24/EU, číslo, symbol nebo specifický údaj přiřazený fyzické osobě za účelem její jedinečné identifikace pro zdravotnické účely, informace získané během provádění testů nebo vyšetřování části těla nebo tělesných látek, včetně z genetických údajů a biologických vzorků, a jakékoliv informace například o nemoci, postižení, riziku onemocnění, anamnéze, klinické léčbě nebo fyziologickém či biomedicínském stavu subjektu údajů nezávisle na jejich původu, tedy bez ohledu na to, zda pocházejí například od lékaře nebo jiného zdravotníka, z nemocnice, ze zdravotnického prostředku či diagnostických testů in vitro.“ (b. 35 recitálu GDPR)

Vedení zdravotnické dokumentace dle GDPR

- Relevantní právní povinnost umožňující zpracování osobních údajů při poskytování zdravotní péče a základní podmínky jejího plnění stanoví § 53 a násl. zákona č.372/2011 Sb. o zdravotních službách
- Další podmínky vedení zdravotnické dokumentace stanoví související zvláštní zákony (např. zákon č. 373/2011 Sb., o specifických zdravotních službách)
- Podrobné podmínky vedení zdravotní dokumentace včetně jejích obsahových náležitostí, zvláštních podmínek jejího uchování, postupu elektronizace, dob uchování, procesu vyřazování, jakož i minimální obsah některých samostatných součástí zdravotnické dokumentace stanoví prováděcí vyhláška MZ č. 98/2012 Sb., o zdravotnické dokumentaci
- Pozor - vyhláška č. 98/2012 Sb. byla změněna novelou č.137/2018 Sb. s částečnou účinností od 24. 7. 2018 a ve zbylé části od 1.11.2018

Vedení zdravotnické dokumentace dle GDPR

- Změna vyhlášky č. 98/2012 Sb. provedena její novelou č.137/2018 Sb. upravuje:
 - Obsahové náležitosti zdravotnické dokumentace
 - Způsob pořizování zápisů do zdravotnické dokumentace
 - Minimální obsah některých samostatných součástí zdravotnické dokumentace
 - Dobu uchovávání vybrané zdravotnické dokumentace
 - Proces vyřazování zdravotnické dokumentace
 - Postup převádění zdravotnické dokumentace v listinné podobě do elektronické podoby
 - Převádění zdravotnické dokumentace v listinné podobě do elektronické podoby
- Převádění zdravotnické dokumentace z listinné do elektronické podoby musí být prováděno postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost obsahu, čitelnost dokumentu a bezpečnost procesu převádění

Kybernetická bezpečnost ve zdravotnictví a GDPR

- Elektronizace zdravotnické dokumentace a další projekty a výzvy, jako jako zavedení elektronické preskripce, telemedicína či mHealth nutně vyžadují vyšší míru automatizace zpracování osobních údajů při poskytování zdravotní péče
- Lékaři v postavení správců jsou povinni provést vhodná technická a organizační opatření pro zajištění úrovně zabezpečení odpovídající danému riziku dle čl. 32 odst. 1 GDPR
- Poskytovatelé zdravotních služeb, nebo na základě jejich pokynů činní dodavatelé v postavení tzv. zpracovatelů osobních údajů, se čím dál častěji stávají cílem různých forem kybernetických útoků
- Aspekt kybernetické bezpečnosti jsou nuceni ve své činnosti zohledňovat všichni poskytovatelé zdravotních služeb včetně jednotlivých lékařů, aniž by v této oblasti byli nutně přímo regulováni zvláštní právní úpravou

Závěr

Jak Ministerstvo zdravotnictví ČR odhadlo v roce 2017 v metodice *Jak implementovat v ambulantní sféře nařízení Evropského parlamentu a Rady (EU) 2016/679* nejčastější chyby a rizika, která lze při práci s osobními údaji očekávat v ambulancích a v primární praxi: „Tedy hlavní a nejzávažnější chyby zcela jistě zahrnují nekontrolovanou práci s dokumentací pacientů (nechráněné a nekontrolované přístupy), nezabezpečenou komunikaci obsahující osobní a citlivé údaje pacientů či rizika vyplývající z používaných IT systémů (nelegální software, chybějící elementární zabezpečení, apod.)“

http://www.mzcr.cz/Legislativa/obsah/implementace-gdpr_3805_11.html

KRITICKÉ MOMENTY
ZPRACOVÁNÍ
OSOBNÍCH ÚDAJŮ
DLE GDPR PŘI
POSKYTOVÁNÍ
ZDRAVOTNÍ PÉČE

Děkujeme!

KMVS, advokátní kancelář, s.r.o.