# Informace k implementaci GDPR

**Uvádíme některé informace v souvislosti s obecným nařízením Evropského parlamentu a rady (EU) 2016/679 o ochraně osobních údajů a současně i možné vzory některých dokumentů.**

**V současné době chybí prováděcí zákon České republiky k obecnému nařízení (EU) 2016/679, které je účinné od 25. května 2018. Teprve tento zákon stanoví skutkovou podstatu možných deliktů v rámci ochrany osobních údajů a výši sankcí za tyto delikty. Do doby než nabyde tento zatím připravovaný zákon účinnosti, nelze žádné sankce v souvislosti s implementací GDPR v ČR ukládat.**

**Poskytovatel zdravotní služby rozhodně nepotřebuje písemný souhlas pacienta s tím co je povinen vést podle zákona, případně dalších právních předpisů. Zejména by bylo nesmyslné vyžadovat souhlas s tím, že může nadále vést zdravotnickou dokumentaci pacienta.** Pokud však poskytovatel zdravotní služby vede mimo zdravotnickou dokumentaci ještě nějaké další osobní údaje obsahující jiné údaje o pacientech, které nevyplývají z právních předpisů, pak je povinen vyžádat si souhlas s tímto evidováním osobních údajů pacientů. Tedy pokud vede něco, co neukládá výslovně právní předpis je třeba souhlas pacienta v písemné formě vyžádat. Může jít například o evidenci smlouvy o poskytování dohodnutých služeb nehrazených ze zdravotního pojištění. Řada poskytovatelů poskytuje na základě písemné smlouvy pacientům tyto služby a smlouvu pochopitelně evidují, přičemž tato smlouva není již povinnou součástí zdravotnické dokumentace, proto k tomu aby osobní údaje uvedené v této smlouvě mohl poskytovatel evidovat případně zpracovávat, potřebuje již souhlas tzv. subjektu údajů, tedy pacienta.

**Nařízení EU však současně dává právo tzv. subjektu údajů v našem případě pacientovi namítat, že osobní údaje, které jsou o něm správcem osobních údajů (ošetřujícím lékařem) vedeny jsou nepřesné, chybné, nebo nepravdivé**. Vznese-li subjekt údajů, v našem případě pacient, takovou námitku, musí se tím správce osobních údajů zabývat a vyřešit ji ať již tak, že uvede nepřesné nebo nepravdivé osobní údaje do správného stavu na základě vznesené námitky, nebo námitku odmítne a odmítnutí odůvodní. Subjekt údajů, v našem případě pacient, se v tomto případě může obrátit na Úřad pro ochranu osobních údajů, pokud jeho žádosti o odstranění nepřesností nebo nepravdivých údajů ve zdravotnické dokumentaci nebude vyhověno. Subjekt údajů, v našem případě pacient, by měl být rovněž zpracovatelem osobních údajů (poskytovatelem - lékařem) informován o tom kdo má přístup k jeho osobním údajům a jak jsou tyto osobní údaje chráněny.

## Co z toho konkrétně pro poskytovatele zdravotních služeb vyplývá:

**Doporučujeme zavést si do 25. května 2018 jednu složku, ve které budou seřazeny písemnosti týkající se implementace nařízení EU o ochraně osobních údajů v příslušném zdravotnickém zařízení.** Tato složka by měla obsahovat informace pro pacienty o zpracování jejich osobních údajů. Tyto informace by měly být k nahlédnutí každému pacientovi, který o to požádá. V čekárně ordinace nebo na jiném vhodném místě by bylo vhodné zveřejnit, že každý pacient má právo nahlédnout do informací o tom, jaké jsou o něm vedeny poskytovatelem zdravotních služeb osobní údaje a jakým způsobem jsou tyto osobní údaje zabezpečeny. Příslušná složka by tedy měla obsahovat informace pro pacienty buď o tom že o nich jsou vedeny konkrétní údaje vyplývající ze zákona o zdravotních službách a vyhlášky o zdravotnické dokumentaci a jaké konkrétní údaje to jsou s tím, že je možno podle zákona do zdravotnické dokumentace i nahlížet a činit si z ní fotokopie. Dále by měla jako další dokument v uvedené složce být uvedena analýza osobních údajů, které poskytovatel zdravotních služeb vede a způsob jakým je chrání, včetně poučení a proškolení zaměstnanců zdravotnického zařízení o ochraně osobních údajů a implementaci nařízení EU o ochraně osobních údajů v konkrétním zdravotnickém zařízení.

Součástí této analýzy nebo samostatným dokumentem by mělo být i zhodnocení rizik, tedy interní revize osobních údajů a úvaha o tom jaká hrozí bezpečnostní rizika z hlediska neoprávněného napadení osobních údajů a jakými prostředky je vzniku těchto rizik bráněno, případně jaký bude postup v případě, že by příslušné bezpečnostní riziko nastalo.

**Posílání lékařských zpráv a nálezů pacientům elektronickou cestou** je možné v případě, že o to pacient požádá a písemné nejlépe vlastnoručním podpisem nebo alespoň emailovou zprávou z emailu, o kterém lékař bezpečně ví, že patří pacientovi, potvrdí, že si přeje právě na tento email zasílat lékařské zprávy a nálezy, případně tímto způsobem komunikovat s ošetřujícím lékařem a bere na vědomí, že tato emailová komunikace není nijak zabezpečena proti případnému zneužití.

**Poštovní spojení mezi poskytovatelem zdravotní služby a pacientem** je možné s využitím subjektu, který má licenci k poskytování poštovních doručovatelských služeb zejména České pošty i bez výslovného souhlasu pacienta, přičemž postačí zasílání poštovních zásilek tzv. „obyčejnou poštou“ netřeba odesílání doporučeně. Zaslání jakékoli zprávy či písemnosti pacientovi poštou není tedy porušením práva na ochranu jeho osobních údajů. Totéž platí, pokud jsou poštou zasílány lékařské zprávy a nálezy mezi poskytovateli zdravotních služeb např. poskytovatel komplementu zasílá ošetřujícímu lékaři výsledky vyšetření, nebo radiologické pracoviště výsledky zobrazovacích metod, apod.

**Emailová komunikace mezi poskytovateli zdravotních služeb obsahující osobní údaje o pacientech** však chráněna být musí a je třeba v tomto směru uzavřít smlouvu s kvalifikovanou společností, která poskytuje služby v oblasti informačních technologií, aby se zavázala, že způsobem odpovídajícím

úrovni evropských standardů zabezpečí bezpečný přenos údajů o pacientech mezi poskytovateli zdravotních služeb emailem. Totéž platí i o závazku poskytovatele informačních technologií, který případně spravuje počítačovou techniku příslušného soukromého lékaře, aby se zavázal k řádné ochraně osobních údajů vedených na příslušných elektronických nosičích o pacientech na standardní evropské úrovni.

**Ve vztahu k zaměstnancům poskytovatele zdravotních služeb a dalším osobám, které na základě jakéhokoli právního titulu přichází do styku s osobními údaji pacientů,** je třeba pamatovat na důsledné poučení těchto osob o povinnosti chránit osobní údaje pacientů, zachovávat mlčenlivost o všech skutečnostech, o kterých se tyto osoby dozvěděly v souvislosti s osobními údaji o pacientech, nakládat s jakýmikoli údaji o zdravotním stavu pacientů jako s chráněnými osobními údaji podléhajícími povinné mlčenlivosti a povinnosti chránit jak písemnou tak elektronickou dokumentaci pacientů. Rovněž vzor tohoto dokumentu o poučení zaměstnanců poskytovatele případně dalších spolupracujících osob, které se mohou dostat do kontaktu s osobními údaji pacientů, bude zveřejněn počátkem května roku 2018 na webových stránkách České lékařské komory www.lkcr.cz .

**V této souvislosti je třeba pamatovat i na řádné zabezpečení jak papírové tak elektronicky vedené zdravotnické dokumentace o pacientech, která by měla být zabezpečena proti vniknutí neoprávněných osob.** Není stanoveno jakým způsobem, zda skříň, kde je uložena zdravotnická dokumentace, musí být uzamčena, nebo zda musí být uzamčena ordinace či prostory zdravotnického zařízení, ani není stanoveno, jaké má být technické zabezpečení ordinace, či zdravotnického zařízení. Je to na rozhodnutí správce – tedy provozovatele ordinace poskytovatele zdravotnických služeb, avšak mělo by být přiměřené tak, aby bránilo tomu, aby se kdokoli nepovolaný dostal ke zdravotnické dokumentaci nebo k jiným osobním údajům vedených o pacientech.

**Nelze zapomenout ani na osobní údaje o zaměstnancích poskytovatele zdravotní služby a jejich ochranu.** Zaměstnanec zdravotnického zařízení by měl být rovněž informován o tom, jaké osobní údaje o něm vede jeho zaměstnavatel a z jakého důvodu. Je pochopitelné, že osobními údaji o zaměstnanci bude pracovní smlouva případně mzdový výměr a veškerá poučení jak o ochraně osobních údajů a povinné mlčenlivosti, tak i údaje o proškolení z bezpečnostních, protipožárních a dalších předpisů. Součástí těchto osobních údajů o zaměstnanci mohou být i údaje o jeho kvalifikaci a fotokopie příslušných dokumentů osvědčujících tuto kvalifikaci zaměstnance. Zaměstnavatel by však rozhodně neměl vést žádné osobní údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, nebo o členství v odborech a zpracování genetických údajů nebo biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o sexuálním životě či sexuální orientaci fyzické osoby, což výslovně zakazuje článek 9 nařízení EU o ochraně osobních údajů. Údaje o zdravotním stavu zaměstnance mohou být vedeny pouze v rozsahu, které stanoví příslušný právní předpis – tedy posudek lékaře poskytujícího pracovně lékařské služby o způsobilosti, omezené způsobilosti, či nezpůsobilosti zaměstnance vykonávat příslušné zaměstnání.

**Shrnutí:**

**1) V souvislosti s implementací nařízení (EU) 2016/679 od 25. května 2018 nehrozí poskytovatelům zdravotních služeb žádné sankce až do doby než konkrétní zákon České republiky nabude účinnosti a stanoví, za jaké jednání lze jaké sankce ukládat.**

**2) Nařízení EU o ochraně osobních údajů nestanoví žádné konkrétní způsoby, jak je poskytovatel zdravotních služeb povinen chránit osobní údaje, které vede o pacientech. Je na úvaze každého poskytovatele - správce osobních údajů, jak rozumně a přiměřeně ve vlastních podmínkách bude tyto údaje chránit.**

**3) Lze doporučit, aby každý poskytovatel zdravotní služby do 25. května 2018 zavedl písemnou složku (šanon) nadepsaný jako „Implementace nařízení EU o ochraně osobních údajů u poskytovatele zdravotní služby“, ve které bude shromažďovat zejména následující dokumenty:**

a) **interní analýza osobních údajů zpracovávaných poskytovatelem zdravotní služby – zda zpracovává pouze osobní údaje stanovené právními předpisy nebo kromě údajů stanovených právními předpisy zpracovává ještě jiné osobní údaje a k jejich zpracování má souhlas subjektů údajů (pacientů).**
b) **Jak přiměřeně jsou tyto údaje chráněny před zneužitím a jaká hrozí tzv. bezpečnostní rizika – zejména údaje o zabezpečení papírové zdravotnické dokumentace v ordinaci a údajů vedených o pacientech na elektronických nosičích výpočetní techniky.**
c) **Informace pro pacienty o tom, které osobní údaje jsou o nich zpracovávány (údaj o tom, že tyto informace jsou u poskytovatele k dispozici pacientům k nahlédnutí, by měl být vyvěšen na viditelném místě v čekárně nebo v ordinaci).**
d) **Formulář pro ohlášení porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů.**
e) **Záznam o proškolení zaměstnanců a dalších spolupracujících osob např. zdravotní sestry, uklízečky, recepční a dalších o povinné mlčenlivosti a ochraně osobních údajů, včetně podpisů proškolených osob.**
f) **Smlouva o zpracování osobních údajů a jejich náležitém zabezpečení s dodavateli informačních technologií a s firmami, které spravují informační technologie poskytovatele zdravotní služby, nebo dodatek ke stávající smlouvě.**
g) **Případný souhlas pacienta se zasíláním lékařských zpráv a nálezů emailovou poštou a případný souhlas pacienta s vedením dalších osobních údajů o jeho osobě, které nevyplývají z právních předpisů (např. smlouvy o poskytování dohodnutých služeb nehrazených ze zdravotního pojištění).**
h) **Seznam osobních údajů, které vede poskytovatel zdravotních služeb o svých zaměstnancích a doklad o tom, že s touto skutečností byli zaměstnanci seznámeni.**

**Vzory příslušných dokumentů nelze bezmyšlenkovitě převzít, ale uvážit zda příslušný vzor odpovídá konkrétním podmínkám poskytovatele, případně jej konkretizovat na vlastní podmínky. Tyto vzory bude možno nalézt od května 2018 na webových stránkách www.lkcr.cz a v příloze je přikládáme**.