GDPR v praxi

Jednání právníků komory s vedoucími pracovníky Úřadu pro ochranu osobních údajů

Právní kancelář ČLK iniciovala schůzku se zástupci Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ"), neboť ÚOOÚ bude hrát zásadní roli v kontrole dodržování obecného nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR). Podnětná schůzka přinesla řadu informací, s nimiž vás dále, v souvislosti s blížícím se dnem účinnosti obecného nařízení (25. května 2018), seznámíme.

Jde o obecné nařízení, které bude postupně implementováno s ohledem na konkrétní podmínky. Stanovisko "co dělat" se bude postupně vyvíjet praxí.

Obecné nařízení o ochraně osobních údajů (také jen „nařízení") má, jak již z názvu normy vyplývá, obecný charakter. V tomto smyslu je nutno vnímat i obsah tohoto nařízení, který v obecné rovině stanoví podmínky pro ochranu osobních údajů, ale současně dává široký interpretační prostor pro jednotlivá ustanovení a taktéž umožňuje členským státům přijetí vlastní (národní) právní úpravy, která bude v souladu s tímto nařízením. Sám úřad konstatoval, že se nejedná o žádnou revoluci pro ty subjekty, které doposud postupují dle platné právní úpravy. Tímto měli zástupci ÚOOÚ na mysli zejména lékaře, které čekají pouze dílčí změny, jež jsou přirozené téměř při každé legislativní změně. Jinak řečeno slovy náměstka ministra zdravotnictví pro legislativu a právo a předsedy revizní komise Společnosti medicínského práva ČLS JEP na konferenci Společnosti medicínského práva JUDr. Policara: „Jde prakticky o to, udělat si doma pořádek."

Rovněž jsme se shodli, že řada firem pořádajících kurzy a přednášky na toto téma, vytváří neopodstatněný tlak s cílem vyvolat v posluchačích pocit, že nesplnění nařízení do data nabytí účinnosti povede k ukládání likvidačních pokut, přičemž tyto firmy vždy nabízí spásné řešení spočívající ve zpracování informací, které budou v souladu s nařízením, samozřejmě za nemalý finanční obnos. **Jak již bylo výše řečeno, jedná se v současné chvíli o obecnou normu, která se bude postupně vyvíjet a jednotlivé instituty budou zpřesňovány a vykládány s ohledem na aktuální potřeby a stav společnosti. Tento kontinuální proces přirozeně vede k tomu, že není potřeba zásadním způsobem měnit současný chod ordinace. Pouze je potřeba přijmout některá dílčí opatření, které ve většině případů korespondují s doposud platným zákonem č. 101/2000 Sb., o ochraně osobních údajů, zákonem č. 372/2011 Sb. o zdravotních službách (zejména částí týkajících se povinné mlčenlivosti a zdravotnické dokumentace) a vyhláškou č. 98/2012 Sb. o zdravotnické dokumentaci. Závěr tohoto úvodu je tedy jednoznačný, nespěchat, nedělat unáhlená rozhodnutí a nepodléhat tlaku firem či mediálním dezinformacím.**

Není stanovena žádná závazná konkrétní písemná forma

Obecnost nařízení je spojena s volností formy, jakou má lékař toto nařízení implementovat v rámci své ordinace. Není tedy stanovena závazná forma, předepsané formuláře apod. V některých případech je obecně stanoven rozsah informací, které musí dokument v souvislosti s nařízením obsahovat. Příkladem může být informace pro subjekty osobních údajů, což je nově zavedený

institut, kdy každý pacient bude mít právo žádat o sdělení, jaké informace o něm lékař shromažďuje a současně je každý lékař povinen o těchto o něm vedených informacích pacienta vhodným způsobem informovat, buďto na webu, v čekárně vyvěšením těchto informací nebo jiným způsobem. Právní kancelář ČLK postupně zpracuje vzor této informace.

Otázka pověřence pro ochranu osobních údajů

Řada dotazů směřuje k institutu tzv. pověřence pro ochranu osobních údajů, nejčastěji zda jsou povinni pověřence ustanovit či nikoliv. Tady se zcela jasně projevuje obecnost nařízení, které nedává zcela jasnou odpověď pro oblast zdravotnictví. Pracovní skupina WP29 výslovně uvádí, že pověřence nemusí mít ambulance o jednom lékaři a jedné zdravotní sestře. K dalším možnostem, tj. několik lékařů či zaměstnání několika zdravotnických pracovníků se WP29 nevyjádřila. Zájemce o tuto problematiku lze odkázat na webové stránky ÚOOÚ (www.uoou.cz), který zveřejňuje stanoviska pracovní skupiny WP29 i v českém jazyce. Tato problematika byla projednána se zástupci ÚOOÚ, s ohledem na neexistující závazný výklad či jiný pokyn, zvažuje ÚOOÚ stanovení hranice prostřednictvím počtu lékařů, kdy jako ideální se jeví počet 9 lékařů. V těchto případech by nebylo nutno ustanovovat pověřence pro ochranu osobních údajů. Další zmíněnou možností pro zajištění pověřence bylo kritérium podle počtu pacientů, což se nejeví jako zcela ideální postup s ohledem na specifika registrujících lékařů a ambulantních specialistů. Bude tedy potřeba vyčkat a do této doby se domníváme, že běžné ordinace pověřence pro ochranu osobních údajů jmenovat nemusí. Tento závěr se nevztahuje na polikliniky, nemocnice apod. V případě ustanovení pověřence je potřeba tuto skutečnost oznámit ÚOOÚ. Pokud poskytovatel pověřence neurčí, což bude asi ve většině případů běžných soukromých praxí, kdy zdravotní služby poskytuje méně než deset lékařů, není nutno ÚOOÚ hlásit, že pověřenec nebyl ustanoven, ale je třeba interním dokumentem zdůvodnit, proč poskytovatel pověřence nepotřebuje.

Smlouva se zpracovatelem osobních údajů

Lékař je při poskytování zdravotní péče ve vztahu k nařízení správcem osobních údajů. Má-li externí firmu, která mu data o pacientech spravuje, tzv. zpracovatele, je důležité, aby byla revidována smlouva s touto externí firmou. Firma by měla mít uloženou povinnost postupovat vždy v souladu s nařízením, dále by měla smlouva obsahovat ustanovení o zabezpečení ochrany osobních údajů na úrovni evropských standardů, případně závazek zpracovatele spočívající v maximálním zajištění těchto dat. Je potřeba si uvědomit, že prvotně nese odpovědnost vždy správce, tedy lékař, který data prostřednictvím zpracovatele uchovává.

Interní revize zpracovávaných osobních údajů

Žádný lékař se nevyhne interní revizi spočívající v sestavení kategorií osobních údajů, které jako správce zpracovává. Záznamy o činnostech zpracování by měly obsahovat rozsah osobních údajů, které lékař zpracovává (např. jméno, příjmení, rodné číslo, údaje o zdravotním stavu apod.), dále je potřeba uvést jak a kde tyto údaje zpracovává (např. zdravotnická dokumentace), jaké má pro zpracování oprávnění (např. zpracování je povinnost vyplývající ze zákona, smlouvy s pacientem apod.) a za jakým účelem tyto informace zpracovává. Této revizi by měl lékař věnovat pozornost, neboť se jedná o zásadní dokument, který musí odpovídat skutečným poměrům v konkrétní ordinaci. Důležitým dokumentem, který z této interní revize vyplyne, je informace o zpracování osobních údajů pro subjekty údajů (pacienty) viz výše, která by měla obsahovat identifikaci správce, účel zpracování osobních údajů, důvody, pro které jsou osobní údaje zpracovávány, kdo je příjemcem těchto osobních údajů a jaké mají práva subjekty údajů (ti o kterých jsou osobní údaje vedeny). **Půjde tedy o to sepsat, jaké lékař vede dokumenty obsahující osobní údaje pacientů (jejich identifikaci a údaje o nich), zda jsou to pouze dokumenty vyplývající z právních předpisů (zdravotnická dokumentace, hlášení zdravotním pojišťovnám pro účely vykázání poskytnuté péče, hlášení NZIS, apod), nebo zda**

vede o pacientech ještě jiné osobní údaje, které již nemá právní povinnost vést (smlouvy s pacienty například o poskytnutí dohodnutých služeb nehrazených ze zdravotního pojištění, podklady potřebné pro výzkum a vědeckou práci vedené se souhlasem pacienta, apod.). Tyto údaje pak vhodným způsobem (webové stránky, vývěska v čekárně ordinace) sdělit pacientům. Vzorový dokument právní kancelář komory dodatečně zveřejní.

Zhodnocení rizik

Po zpracování revize zpracovávaných osobních údajů bude potřeba vymezit a zhodnotit rizika pro práva a svobody subjektů údajů (v našem případě především pro pacienty a únik údajů o jejich zdravotním stavu). Toto zhodnocení má reflektovat možná rizika, které zpracováním osobních údajů mohou vzniknout a zasáhnout tak do práv pacientů v souvislosti s ochranou osobních údajů. Výše uvedené nezbytné součásti povinné dokumentace je třeba doplnit o záznam o proškolení zaměstnanců a případného vzoru dokumentu pro případ porušení zabezpečení a ohlášení porušení zabezpečení, kdy tento dokument slouží k hlášení bezpečnostních incidentů, které mohou mít vliv na práva subjektů osobních údajů, například hackerský útok, krádež výpočetní techniky či vloupání do zabezpečené kartotéky apod. Tento bezpečnostní incident je každý zpracovatel povinen nahlásit ÚOOÚ ve lhůtě 72 hodin. Je však potřeba vždy důsledně posoudit, do jaké míry jsou práva subjektů osobních údajů ohrožena, neboť netřeba každý incident ÚOOÚ hlásit. Vždy bude záležet na míře ohrožení. Opět se jedná o obecnou formulaci, která bude výkladovou praxi postupně zpřesňována.

I v tomto případě právní kancelář ČLK připraví rámcový dokument.

Proškolení zaměstnanců a závazek spolupracujících subjektů k ochraně osobních údajů a dodržování Nařízení

Lékař jako správce osobních údajů by měl mít zpracováno poučení o povinnosti k ochraně osobních údajů pro všechny své zaměstnance a další osoby, které přichází nebo by mohly přicházet do styku s osobními údaji pacientů. V samotných pracovních smlouvách se zaměstnanci by měl mít ustanovení o tom, že zaměstnanec je povinen chránit osobní údaje pacientů a nakládat s nimi v souladu s Nařízením Evropského parlamentu a Rady 2016/679 a právními předpisy ČR a skutečnost, že zaměstnanec podpisem potvrzuje, že byl o těchto svých povinnostech zaměstnavatelem proškolen. To se v běžné ordinaci může týkat především zdravotních sester, sanitářů, laborantů, ale i uklízeček. Podobně musí poskytovatel zavázat k ochraně osobních údajů všechny své obchodní partnery, dodavatele služeb, apod., kteří ať již z jakýchkoli důvodů přichází do styku s osobními údaji pacientů. To se bude patrně týkat především případného správce IT systému, který se lékaři stará o počítač, ale případně i účetnických firem nebo účetních a firem, které zabezpečují předávání informací o poskytnutých zdravotních službách zdravotním pojišťovnám pro účel úhrady zdravotních služeb z veřejného zdravotního pojištění, pokud lékař takových firem využívá. Ve všech těchto případech by měl být ve smlouvě zakotven výslovný závazek příslušné firmy nebo pracovníka nakládat s osobními údaji pacientů v souladu s Nařízením Evropského parlamentu a Rady 2016/679 a právními předpisy ČR.

Zajištění prostor ordinace a uložení zdravotnické dokumentace i počítačů

S ochranou osobních údajů souvisí i řádné zajištění ordinace, které v drtivé většině splňuje většina lékařů provozujících soukromé praxe. Kartotéka by neměla být běžně dostupná, měla by být uzamykatelná a měla by být umístěna v odpovídajících prostorách. Jako příklad nevhodného umístění kartotéky jsou například prostory čekárny. Rovněž výpočetní technika by měla být opatřena heslem nejen do operačního systému, ale i zdravotnického softwaru, přičemž je žádoucí, aby při opuštění ordinace byl lékař či sestra řádně odhlášeni. Současně by zaměstnanci měli být řádně proškoleni i

v této oblasti. Samostatnou kapitolou bude používání kamerových systémů s ohledem na podmínky stanovené nařízením. K tomu se ještě později vrátíme. Nic zásadně nového však v tomto směru Nařízení nepřináší.

Sdělování výsledků vyšetření pacientům a mezi poskytovateli

Rovněž byla konzultována problematika sdělování výsledků a zdravotních informací pacientům na jejich žádost a po dohodě s nimi prostřednictvím e-mailů či telefonů. V těchto postupech není nutno nic měnit, pokud má lékař s pacientem písemně dohodnutou e-mailovou komunikaci, měl by ho navíc poučit o skutečnosti, že předávání informací probíhá tzv. nezabezpečeným kanálem. Rovněž lze i nadále sdělovat zdravotní informace telefonicky za předpokladu, že bylo s pacientem dohodnuto heslo, pin kód, či obdobný způsob identifikace volajícího.

V případě předávaní zdravotních informací mezi poskytovateli zdravotních služeb a zdravotnickými zařízeními by vždy mělo být zabezpečené prostředí, kterému běžná e-mailová komunikace nevyhovuje. Jako vhodná se jeví komprimace těchto informací za současného silného zaheslování (kombinace velkých a malých písmen a čísel).

Závěr

Z výše uvedeného vyplývá, že s ohledem na obecné nařízení je potřeba zpracovat několik poměrně jednoduchých základních dokumentů, které by měly být uloženy v ordinaci (mohou být i v elektronické podobě). Obsahové náležitosti jednotlivých součástí byly uvedeny blíže, přičemž právní kancelář zpracuje obecné vzory, které si pak každý poskytovatel doplní dle svého aktuálního stavu.

Zájemce o hlubší studium této problematiky lze odkázat na Metodiku Ministerstva zdravotnictví a ÚZIS "Jak implementovat Nařízení Evropského parlamentu a Rady 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů do resortu zdravotnictví", která je zveřejněna na webových stránkách České lékařské komory (www.lkcr.cz).

Závěrem opakujeme, že není potřeba při implementaci nařízení postupovat unáhleně, neboť se jedná o dlouhodobý proces, který se postupně vyvíjí. O případných změnách budeme postupně informovat. Vzhledem ke specifice oblasti soukromých praxí, kdy drtivá většina osobních údajů je získávána v souvislosti s plněním právní povinnosti, lze výše uvedené dokumenty považovat za dostatečný základ implementace nařízení.

JUDr. Jan Mach
ředitel právní kanceláře ČLK

Mgr. Daniel Valášek
právní kancelář ČLK