Kritické momenty zpracování osobních údajů dle GDPR při poskytování zdravotní péče

Respekt k soukromí a potřeba ochrany osobních údajů zejména pacientů nutně provází poskytovatele zdravotních služeb při jejich odborné činnosti takřka každý den. Tak jako právo na úctu, důstojné zacházení, na ohleduplnost, má pacient také právo na respekt k soukromí při poskytování zdravotních služeb v souladu s charakterem poskytovaných zdravotních služeb. Všechna tato práva, která společně s dalšími vyjmenovává v úvodu části čtvrté zákon č. 372/2011 Sb. o zdravotních službách, mají svůj lidskoprávní základ. Článek 10 odst. 2 Listiny základních práv a svobod (dále jen „Listina“) uvádí, že každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Protože k zásahu do soukromí nutně dochází mimo jiné také při neoprávněném shromažďování, zveřejňování nebo jiném zneužíváním údajů, přiznává Listina v článku 10 odst. 3 dotčeným fyzickým osobám výslovně ochranu i proti takovým zásahům. Zatímco konkrétní podmínky ochrany před jednorázovými, resp. nesystematickými zásahy do soukromí jednotlivce stanoví zákon č. 89/2012 Sb. Občanský zákoník, tak v případech, kdy někdo s projevy osobní povahy či jinými informacemi týkajícími se určené nebo určitelné fyzické osoby, které jsou obsaženy v evidenci nebo do ní mají být zařazeny, provádí systematicky nějakou operaci nebo soustavu operací, bylo třeba až donedávna primárně aplikovat zákon č. 101/2000 Sb. o ochraně osobních údajů. Právě tento zákon konkretizuje a rozvádí již zmíněný článek 10 odst. 3 Listiny. Základní lidské právo na ochranu osobních údajů je obdobně zakotveno také na mezinárodní úrovni, zejména pak v článek 8 odst. 1 Listiny základních práv Evropské unie (dále jen „Listina EU“).

S odkazem na článek 8 odst. 1 Listiny EU a s upozorněním na potřebu reagovat na rychlý technologický rozvoj a vlivy globalizace i na oblast zpracování osobních údajů nabylo dne 25. května 2018 účinnosti po více jak dvou letech od svého schválení nařízení Evropského parlamentu a Rady (EU) 2016/679 zkráceně označované jako obecné nařízení o ochraně osobních údajů, nebo jen zkratkou GDPR z anglického General Data Protection Regulation. Tento evropský právní předpis, který představuje poměrně rozsáhlou a komplexní právní regulaci v oblasti ochrany osobních údajů, nevyžaduje na národní přijetí tzv. implementačních předpisů na rozdíl od předešlé směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Zvolená právní forma v podobě nařízení zakládá aplikační přednost tohoto předpisu před právní úpravou jednotlivých členských států, která by s ním mohla být jakkoli v rozporu. Za účelem zajištění jednoty a bezrozpornosti právního řádu nicméně bude v ČR podobně jako i v dalších členských státech EU přijat také zbrusu nový zákon o zpracování osobních údajů a společně s ním i příslušný doprovodný změnový zákon, které nahradí zákon č. 101/2000 Sb. a jejichž cílem je mimo jiné odstranit případné rozpory, nebo přinejmenším nadbytečné duplicity příslušné právní úpravy regulující podmínky zpracování osobních údajů.

Díky své přímé aplikovatelnosti GDPR garantuje rovnocennou ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů a volný pohyb osobních údajů tak, že stanoví stejná základní pravidla pro všechny členské státy Evropské unie. Členským státům je poskytován pouze určitý omezený prostor pro stanovení vlastních pravidel, včetně pravidel pro zpracování zvláštních kategorií osobních údajů. Tzv. adaptační zákon, jak je také někdy označován připravovaný zákon o zpracování osobních údajů, tím pádem obsahuje také ustanovení, jejichž přijetí na národní úrovni GDPR výslovně předpokládá (tj. například využití výjimek, které jsou v nařízení obsaženy). Závěrem je

třeba zdůraznit, že kromě samotné adaptace GDPR, chystaný zákon o zpracování osobních údajů včetně doprovodného zákona současně transponuje ustanovení směrnice (EU)2016/680, která byla přijata společně s GDPR a která upravuje specifickou oblast zpracování osobních údajů justičními a policejními orgány v trestních věcech. Zajištění adaptace českého právního řádu na relevantní ustanovení GDPR včetně řádného fungování nezávislého dozorového úřadu a zejména pak i včasné provedení transpozice zmíněné směrnice (EU)2016/680 jsou povinnostmi ČR vyplývající z jejího členství v EU, jejichž nesplnění by ve svém důsledku mohlo vést i k uložení citelných finančních sankcí.

Co se týče dozoru v oblasti ochrany osobních údajů tento je dle GDPR svěřen primárně národním dozorovým úřadům, tj. v České republice Úřadu pro ochranu osobních údajů (dále jen „ÚOOU"). S již zmíněným ohledem na rostoucí podíl tzv. přeshraničních zpracování v rámci EU, nebo i v celosvětovém měřítku a také za účelem zajištění jednotného uplatňování pravidel GDPR toto nařízení upravuje působnost a pravomoci Evropského sboru pro ochranu osobních údajů (dále jen „Sbor"). Za účelem efektivnějšího uplatňování pravidel GDPR v případech přeshraničního zpracování osobních údajů GDPR také nově zakotvuje institut vedoucího dozorového úřadu.

Kromě podpory vzájemné pomoci a spolupráce mezi dozorovými úřady se GDPR snaží eliminovat roztříštěnost v postupech dle tohoto nařízení a zajistit jeho jednotné uplatňování v celé EU. Klíčové aktivity včetně rozhodovací činnost ze strany národních dozorových úřadů, ale i samotného Sboru, který nahradil nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí označovaný jako Pracovní skupina dle článek 29, nebo jen anglickou zkratkou WP29 (Working party 29), jsou podřízeny tzv. mechanismu jednotnosti. Mechanismus jednotnosti je založen na povinné spolupráci jednotlivých dozorových úřadů, případně i samotné Komise EU, a zahrnuje úpravu postupů pro vydávání stanovisek, řešení sporů či naléhavých případů a samozřejmě také výměnu informací mezi dozorovými úřady. I přes veškeré změny v organizaci dozoru nad dodržováním GDPR v rámci EU toto nařízení i nadále předpokládá, že každá fyzická nebo právnická osoba má právo na účinnou soudní ochranu ze strany příslušného vnitrostátního soudu proti rozhodnutím dozorového úřadu, která vůči ní zakládají právní účinky.

GDPR přebírá v základu řadu klíčových definic ze směrnice 95/46/ES a podobně jako již dříve uplatňované zásady zpracování osobních údajů, tyto dále rozvíjí ve snaze o nastavení pravidel, která lépe reflektují zejména technologický posun ve způsobu a podmínkách zpracování osobních údajů v globalizovaném světě.

Za nejvýznamnější systémové změny bývá označováno komplexní promítnutí dosud spíše jen nepřímo a dílčím způsobem uplatňovaných principů záměrné a standardní ochrany osobních údajů také někdy označované anglickým spojením *privacy by design* a zejména pak také prosazení přístupu založeného na riziku neboli tzv. *risk based approach*. Princip záměrné a standardní ochrany zdůrazňuje potřebu toho, aby již při samotném vývoji a koncipování produktů, služeb či aplikací, při jejichž využití bude docházet ke zpracování osobních údajů, bylo zohledněno právo na ochranu údajů a brán náležitý ohled zejména na stav techniky s cílem zajistit, aby budoucí správci a zpracovatelé mohli plnit své povinnosti v oblasti ochrany údajů v souladu s GDPR a tím i chránit soukromí dotčených subjektů údajů. Oproti tomu přístup založený na riziku průřezově relativizuje některé povinnosti správců a zpracovatelů, včetně finanční náročnosti jejich plnění, a to v závislosti na riziku,

které implikuje konkrétní činnost zpracování osobních údajů, ať už s ohledem na rozsah či povahu zpracovávaných osobních údajů nebo použité technologie.

Aby bylo možné označit jakoukoli činnost, která má charakter zpracování osobních údajů za oprávněnou, musí být primárně dodržena zásada zákonnosti zpracování osobních údajů, tj. takové zpracování údajů musí být založeno na některém z právních titulů, který stanoví GDPR a který musí odpovídat předem stanovenému účelu zpracování údajů. Jedině při zcela objektivním zodpovězení otázky, za jakým účelem má docházet ke shromažďování, zveřejnění či jakékoli jiné relevantní operaci s osobními údaji fyzických osob, je možné takovou činnost podřadit pod již zmíněný zákonný titul. Rozmanitost titulů pro zpracování dle GDPR, které navíc dále rozlišuje případy zákonného zpracování řekněme prostých osobních údajů a případy, kdy předmětem zpracování mají být tzv. zvláštní kategorie osobních údajů (dříve označované jako citlivé údaje), reflektuje značně široké možnosti toho, z jakých důvodů může v praxi docházet ke zpracování osobních údajů fyzických osob. Pro možné splnění všech požadavků kladených GDPR na konkrétní činnost zpracování osobních údajů je také klíčové členění titulů na případy, pro které je třeba získat předem informovaný a někdy dokonce výslovný souhlas dotčeného subjektu osobních údajů nebo jeho oprávněného zástupce a případy, kdy takového souhlasu není třeba.

GDPR klade velký důraz také na transparentnost zpracování údajů ve vztahu správce údajů s dotčenými subjekty údajů. Praktické uplatnění této zásady vyžaduje, aby všechny informace určené veřejnosti nebo každému jednotlivému subjektu údajů byly stručné, snadno přístupné a srozumitelné, podávané za použití jasných a jednoduchých jazykových nebo ve vhodných případech i jiných prostředků. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty také ústně, a to za předpokladu, že bude dostatečně zajištěno prokázání jeho identity. Informovanost subjektů o tom, kdo a za jakých podmínek zpracovává jejich údaje je klíčovým předpokladem pro možnost uplatnění práv těchto subjektů, která jim GDPR přiznává v širším rozsahu, než tomu bylo kdykoli dříve. Zvláštního ohledu při poskytování informací by se dle GDPR mělo dostat také dětem.

Kromě samotné zákonnosti, korektnosti a transparentnosti zpracování však GDPR vyžaduje, aby jakékoli zpracování osobních údajů podléhající tomuto nařízení vyhovovalo současně všem korektivům, které vyplývají z řady dalších zásad. Mezi tyto zásady GDPR výslovně řadí požadavek, aby zpracování bylo slučitelné s výslovně vyjádřenými a legitimní účely, aby byl minimalizován rozsah jeho provádění, aby byla zajištěna přesnost zpracovávaných údajů a na nezbytné minimum omezená doba uložení osobních údajů. V kontextu velkého rozvoje elektronizace zpracování věnuje GDPR zvýšenou pozornost také zásadě zajištění důvěrnosti a integrity údajů pomocí vhodných technických nebo organizačních opatření. Výčet zásad výslovně uvedených v článku 5 GDPR zakončuje požadavek, aby každý správce zajistil dodržení výše uvedených zásad a současně byl také schopen jejich dodržení doložit, což je zjednodušeně označováno jako tzv. zásada odpovědnosti.

Protože předmětem tohoto výkladu není podrobný rozbor kompletní problematiky ochrany osobních údajů, jak jí nově upravuje GDPR, zaměříme se nyní v dalším výkladu pouze na vybraná specifika zpracování osobních údajů při poskytování zdravotní péče. Jak vyplývá z úvodní obecné části, dodržení povinností v oblasti zpracování osobních údajů stanovených GDPR ve spojení s dalšími případnými právními předpisy je primární odpovědností správce, a to ve vztahu ke všem činnostem, pro které zpravidla sám lékař určuje účely a prostředky zpracování osobních údajů. Nutnou podmínkou pro dosažení souladu s GDPR je pro lékaře, který je správcem osobních údajů, 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 a jak jsou případně likvidovány.

V souvislosti s poskytováním zdravotní péče ambulantním lékařem je takto možné identifikovat hned několik více či méně nevyhnutelných činností, při kterých dochází ke zpracování osobních údajů pacientů i dalších osob, ať už jsou to osoby blízké pacientům, zaměstnanci lékaře nebo např. jeho obchodní partneři včetně dalších lékařů či jiných zdravotnických odborníků. 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, při vedení personální a mzdové agendy, při výzkumné činnosti včetně např. klinických hodnocení a další.

Jednoznačně dominantní a současně i nejrizikovější zpracovatelskou činností kontrolovanou lékařem při poskytování zdravotní péče však zůstává vedení zdravotnické dokumentace, která zahrnuje primárně, ale nikoli výlučně, osobní údaje pacienta. Údaje o pacientech v nemalém rozsahu navíc v tomto případě spadají dle GDPR mezi zvláštní kategorie osobních údajů. Identifikace právního základu (titulu) pro toto zpracování nepředstavuje zásadní problém. Jedná se o zpracování osobních údajů, které je nezbytné pro splnění právní povinnosti správce, jak to předpokládá článek 6 odst. 1 písm. c) GDPR, neboť vedení zdravotnické dokumentace je lékaři uloženo výslovně zákonem č. 372/2011 Sb. o zdravotních službách, konkrétně ustanovením §53 odst. 1. GDPR pro tento případ stanoví zcela logicky také výjimku ze zákazu zpracování zvláštních kategorií osobních údajů, konkrétně tedy údajů o zdravotním stavu pacienta, a to v článku 9 odst. 2 písm. h). Tentýž článek ve svém třetím odstavci stanoví specifický požadavek, dle něhož zvláštní kategorie osobních údajů mohou být zpracovávány pro účely uvedené v odst. 2 písm. h) pouze pracovníkem vázaným služebním tajemstvím nebo na jeho odpovědnost podle práva EU nebo členského státu nebo pravidel stanovených příslušnými vnitrostátními orgány nebo jinou osobou, na niž se rovněž vztahuje povinnost mlčenlivosti podle práva EU nebo členského státu nebo pravidel stanovených příslušnými vnitrostátními orgány. Lékař, stejně jako další zdravotničtí pracovníci tradičně splňují uvedený požadavek mlčenlivosti. Pro praxi lékaře však je podstatné, že členské státy mohou dle článku 9 odst. 4 GDPR zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu. Údaje o zdravotním stavu vymezuje GDPR v článku 4 odst. 15 jako osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu, a blíže pak tuto definici rozvádí v bodě 35 recitálu GDPR.

Základ právní povinnosti umožňující zpracování osobních údajů při poskytování zdravotní péče i bez nutnosti získání předchozího souhlasu pacienta s takovým zpracováním tedy stanoví společně s dalšími podmínkami vedení zdravotnické dokumentace §53 a násl. zákona č. 372/2011 Sb. o zdravotních službách. Další podmínky vedení zdravotnické dokumentace stanoví související zvláštní zákony, jako je například zákon č. 373/2011 Sb. o specifických zdravotních službách. Podrobné podmínky vedení zdravotní dokumentace včetně jejích obsahových náležitostí, postupu elektronizace, podmínek a dob uchování, procesu vyřazování, jakož i minimální obsah některých samostatných součástí zdravotnické dokumentace stanoví prováděcí vyhláška Ministerstva zdravotnictví ČR č. 98/2012 Sb., o zdravotnické dokumentaci.

Na tomto místě je třeba upozornit, že poměrně brzy po nabytí účinnosti GDPR byla vyhláška o zdravotnické dokumentaci novelizována, a to přijetím vyhlášky MZ č. 137/2018 Sb. v relevantní části účinné od 24. července 2018 a ve zbytku od 1.11.2018. Pozornost tak je třeba věnovat jak změnám obsahových náležitostí zdravotnické dokumentace, tak i některým změnám ve způsob pořizování zápisů do zdravotnické dokumentace. K určitému rozvolnění dochází v souvislosti se zmíněnou novelou v otázce minimálního obsahu některých samostatných součástí zdravotnické dokumentace, jako je informovaný souhlas, odmítnutí poskytnutí zdravotních služeb (neboli revers), záznam o dříve vysloveném přání pacienta nebo souhlas s poskytováním informací. V důsledku zrušení bližších náležitostí těchto záznamů přímo ve vyhlášce bude třeba při jejich vytváření primárně sledovat obecné požadavky uvedené v zákoně o zdravotních službách. Pochopitelně nezbytné úpravy v dříve zavedených postupech a také příslušných informačních systémech bude třeba provést v návaznosti na změny v dobách uchovávání určitých typů zdravotnické dokumentace a také procesu vyřazování zdravotnické dokumentace.

Nicméně do budoucna zůstává pravděpodobně největší výzvou pro lékaře v postavení správců dat, kteří jsou odpovědní za vedení zdravotní dokumentace a tím i zpracování v ní uvedených údajů, otázka elektronizace zdravotní dokumentace. Jedním z cílů citované novely bylo definitivně umožnit lékaři vedení zdravotní dokumentace výhradně v elektronické podobě, což bylo dříve považováno s ohledem na určité požadavky kladené vyhláškou a zákonem jako do jisté míry problematické. Převedení zdravotnické dokumentace nebo jejích částí, které byly pořízeny v listinné podobě a které lékař sám pořídil nebo obdržel, na dokument v elektronické podobě se musí provádět postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost obsahu, čitelnost dokumentu a bezpečnost procesu převádění. Na některá možná úskalí z hlediska ochrany osobních údajů při vedení zdravotnické dokumentace v elektronické podobě se snažil upozornit také ÚOOÚ, a to ve stanovisku č. 3/2015 - *Zpracování osobních údajů v souvislosti s vedením zdravotnické dokumentace*, které zůstává v mnohém relevantní i po účinnosti GDPR. Úřad v závěru tohoto stanoviska uvedl: „*Přestože veřejnosti jsou známy především medializované případy týkající se nalezení zdravotnických dokumentací v listinné formě na místech, která nejsou k jejich uložení určena, lze shledávat vysoké potenciální riziko i v případech zdravotnických dokumentací vedených ve formě elektronické, a to zejména v nastavení přístupu jednotlivých oprávněných osob do zdravotnické dokumentace u větších poskytovatelů zdravotních služeb (především velkých nemocnic).*“

Závěrem se ještě krátce zastavme u otázky kybernetické bezpečnosti v odvětví zdravotnictví a GDPR. Elektronizace zdravotnické dokumentace, společně s projekty jako zavedení elektronické preskripce či elektronických zdravotních knížek nebo i další oblasti jako například rozvoj telemedicíny či mHealth, které nutně vyžadují vyšší míru automatizace zpracování osobních údajů při poskytování zdravotní péče, přináší nepochybně řadu výhod a pozitiv, jak na straně státu a většiny poskytovatelů zdravotních služeb, tak i samotných pacientů. Na druhou stranu je třeba stále pamatovat, že je to právě povaha a hodnota dat, s nimiž lékaři pracují a které nevyhnutelně vypovídají především o zdravotním stavu pacientů, co v souladu s přístupem založeným na riziku klade na lékaře, případně zdravotnická zařízení v postavení správců údajů značně vysoké nároky. To se nutně promítá i do povinnosti lékařů s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provést vhodná technická a organizační opatření pro zajištění úrovně zabezpečení odpovídající danému riziku, jak vyplývá z čl. 32 odst. 1 GDPR. Ostatně jsou to právě a stále častěji poskytovatele zdravotních služeb, nebo na základě jejich pokynů činní dodavatelé

v postavení tzv. zpracovatelů osobních údajů, kdo se dle odborných bezpečnostních statistik čím dál častěji stávají cílem různých forem kybernetických útoků.

Dílčí reakci na nežádoucí trend v oblasti kybernetické bezpečnosti projevující se i v oblasti zdravotnictví bylo přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Ten však z počátku spíše jen teoreticky, ale nikoli prakticky umožnoval, aby jím byli přímo regulováni také někteří poskytovatelé zdravotních služeb. To se určitým způsobem změnilo až v souvislosti s novelizací tohoto zákona v rámci implementace Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Nicméně i po této změně zůstávají uvedeným zákonem regulovány z hlediska kybernetické bezpečnosti de facto jen ty největší nemocnice. Metodický pokyn poskytovatelům zdravotních služeb k problematice kybernetické bezpečnosti vydaný v této souvislosti Ministerstvem zdravotnictví je na začátku druhé kapitoly trefně uveden slovy: *„Obecně lze konstatovat, že zabývat se ochranou dat a informací, ať už vymezených legislativou, nebo jiných významných dat a informací organizace, by mělo patřit k základním návykům jakékoliv organizace a ve stále více elektronizovaném světě se tato problematika dostává do centra zájmu jako podmínka kvalitního fungování a dlouhodobého přežití organizace.“* Vhledem k tomu, že s poskytováním zdravotní péče je neodmyslitelně spjato také rizikové zpracování citlivých osobních údajů, které je stále více automatizováno, budou nuceni zohlednit aspekt kybernetické bezpečnosti ve své činnosti všichni poskytovatelé zdravotních služeb včetně jednotlivých lékařů, aniž by v této oblasti byli nutně přímo regulováni zvláštní právní úpravou jako je zákon o kybernetické bezpečnosti. V tomto směru je zcela na místě, když Česká lékařská komora prostřednictvím příslušné sekce GDPR na svých webových stránkách lékaře vyzývá a metodicky instruuje v rámci vzorových dokumentů a dalších informací k tomu, aby kromě zabezpečení dokumentace v elektronické i listinné podobě věnovali při implementaci GDPR náležitou pozornost také zabezpečení (vzdálené) komunikace s pacientem a také komunikace mezi poskytovateli zdravotních služeb navzájem, např. v rámci navazující péče, apod. (https://www.lkcr.cz/gdpr-448.html)

Na úplný závěr tohoto výkladu se nejlépe hodí uvést, jak Ministerstvo zdravotnictví ČR uvedlo v roce 2017 v metodice *Jak implementovat v ambulantní sféře nařízení Evropského parlamentu a Rady (EU) 2016/679* svůj odhad nejčastějších chyb nebo jaká nejčastější rizika 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 zabezpečen, apod.)“* http://www.mzcr.cz/Legislativa/obsah/implementace-gdpr_3805_11.html