HAVLÍČEK & PARTNERS
ADVOKÁTNÍ KANCELÁŘ

Apatyka servis s.r.o.
K pérovně 945/7
10200 Praha 10

V Hradci králové dne 30.7.2019

Průběžná zpráva o vývoji aplikace nařízení Evropského parlamentu a Rady 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/EES - GDPR

Vážení,

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále také jako „obecné nařízení“) vstoupilo do druhého roku své účinnosti.

V souvislosti s účinností obecného nařízení bylo možné zaznamenat citelný nárůst zájmu o právní úpravu na poli ochrany osobních údajů, a to jak ze strany správců, potažmo zpracovatelů osobních údajů, tak ze strany subjektů údajů, tj. osob, jejichž osobní údaje jsou zpracovávány. Účinností obecného nařízení se dále do určité míry upravila povaha Úřadu pro ochranu osobních údajů (dále jen „Úřad“), který na poli ochrany osobních údajů plní dozorovou a kontrolní funkci, ale současně nyní plní i funkci vzdělávací, konzultační a osvětovou.

Skutečnost, že subjekty údajů berou vážně ochranu svých osobních údajů, dokládá znatelný nárůst stížností a podnětů uplatněných u Úřadu pro ochranu osobních údajů v posledním roce. Dle přehledu Úřadu pro ochranu osobních údajů činí počet podnětů ode dne účinnosti obecného nařízení (tj. od 25. května 2018) celkem 3851, zatímco v roce před účinností obecného nařízení přijal Úřad celkem 2385 podnětů. Stížnosti a podněty nejčastěji míří na proces získávání souhlasů pro zpracování osobních údajů, nerespektování práv subjektů údajů, telemarketing a problematiku kamerových systémů.

Na zvýšený zájem subjektů údajů o ochranu svých osobních údajů bezprostředně reaguje i kontrolní činnost Úřadu, který od 25. května 2018 uskutečnil desítky kontrol a uložil statisícové pokuty. Úřad se při své kontrolní činnosti zaměřuje nejen na proces získávání souhlasů se zpracováním osobních údajů, ale i na technická a organizační opatření přijatá jednotlivými správci či zpracovateli osobních údajů, včetně technického zabezpečení přístupu a nakládání s osobními údaji. Jednou z četných oblastí výkonu kontrolní a dozorové pravomoci jsou osobní údaje pacientů, resp. osobní údaje související se zdravotním stavem osob. O uvedeném svědčí

skutečnost, že mezi kontrolovanými osobami byla Nemocnice Tábor, a.s., Oblastní nemocnice Trutnov, a.s., Krajská nemocnice T. Bati, a.s. nebo NaturaMed Pharmaceuticals s.r.o., když právě u Nemocnice Tábor, a.s. bylo předmětem kontroly podezření z možného nahlížení do elektronické zdravotnické dokumentace pacientky a možné pozměňování jejího obsahu neoprávněnými osobami. Kontrola se v tomto případě zaměřila na posouzení úrovně zabezpečení osobních údajů z hlediska jejich fyzického zabezpečení a zabezpečení elektronické zdravotní dokumentace, když dále byly předmětem kontroly technicko-organizační opatření k zajištění ochrany osobních údajů, logování a kontrolní mechanismy včetně školení zaměstnanců co do zpracování osobních údajů.

Je tedy zřejmé, že Úřad bere svoji roli ústředního správního úřadu pro oblast ochrany osobních údajů svědomitě a má k tomuto účelu i potřebné nástroje. K tomuto lze doplnit, že od 24. dubna 2019 vstoupil v účinnost zákon č. 110/2019 Sb., o zpracování osobních údajů, který představuje tzv. adaptační legislativu k obecnému nařízení. Tento zákon na jedné straně doplňuje právní úpravu obecného nařízení a využívá některé výjimky předpokládané obecným nařízením, a na straně druhé utvrzuje institucionální zakotvení Úřadu do právní úpravy ochrany osobních údajů. Lze tedy předpokládat, že po ujasnění institucionálního rámce působnosti Úřadu bude tento pokračovat ve své činnosti o to důrazněji. Vzhledem k četnosti stížností a dotazů subjektů údajů a přijaté právní úpravě adaptačního zákona proto nelze podceňovat implementaci pravidel obecného nařízení do vnitropodnikových předpisů.

Ve vztahu k samotné adaptační legislativě lze shrnout, že pro ochranu osobních údajů v oblasti lékárenství nepředstavuje tento právní předpis žádné zásadní změny. Za zmínku stojí pravidlo obsažené v § 12 zákona o zpracování osobních údajů, které pro případ, kdy je správce povinen oznámit porušení zabezpečení osobních údajů subjektu údajů, může správce takové oznámení provést v omezeném rozsahu nebo jej odložit, je-li to nezbytné a svým rozsahem přiměřené k zajištění chráněného zájmu uvedeného v § 6 odst. 2 zákona o zpracování osobních údajů. Takovým chráněným zájmem může být ochrana práv a svobod osob nebo případné vymáhání soukromoprávních nároků. Správce je však v takovém případě povinen bez zbytečného odkladu oznámit Úřadu, že oznámení subjektu údajů odložil nebo jej provedl v omezeném rozsahu, a musí uvést alespoň základní informace k osobním údajům, u kterých došlo k porušení zabezpečení, jako účel zpracování, kategorii osobních údajů a možná rizika pro práva a svobody subjektů údajů. Dalším ustanovením zákona o zpracování osobních údajů dotýkajícím se činnosti lékáren jakožto správců, kterým povinnost zpracovávat osobní údaje vyplývá ze zákona, je § 8 citovaného zákona. Toto ustanovení umožňuje správcům, kteří zpracovávají osobní údaje na základě zákonné povinnosti, splnit informační povinnost vůči subjektům údajů tak, že informace podle čl. 13 nebo 14 odst. 1,2 a 4 obecného nařízení, poskytnou v rozsahu odpovídajícím jím obvykle prováděnému zpracování osobních údajů způsobem umožňujícím dálkový přístup, tedy například skrze své webové stránky.

V návaznosti na účinnost obecného nařízení je vhodné dále zmínit zřízení Evropského sboru pro ochranu osobních údajů, jehož hlavním posláním je zajištění jednotného uplatňování obecného nařízení. Jedním z posledních vydaných pokynů Evropské sboru je pokyn č. 1/2019 týkající se kodexů chování předpokládaných čl. 40 obecného nařízení a také pokyn č. 4/2018 o akreditaci a

vydávání osvědčení dle čl. 43 obecného nařízení, oba ze dne 04. června 2019. Kodexem chování je možné prokázat soulad s obecným nařízením, přičemž se jedná o dokument obsahující základní zásady, postupy a požadavky na zpracování osobních údajů v konkrétním odvětví (tj. např. lékárenství, pojišťovnictví, bankovní sektor). Přihlášení se k určitému kodexu chování však není v rámci odvětví povinné a jedná se tedy pouze o jednu z variant, jak prokazovat soulad nastavení podnikových předpisů na poli ochrany osobních údajů s obecným nařízením. Důležité je dále uvést, že pokud se správce či zpracovatel přihlásí k dodržování kodexu chování, je povinen podrobit se pravidelnému monitorování kodexu chování nezávislým subjektem. Osvědčením je také možné prokazovat soulad s pravidly uvedenými v obecném nařízení, avšak tato osvědčení se vydávají pro konkrétního správce nebo zpracovatele na dobu, nikoliv pro celé odvětví jako kodexy chování, a jejich platnost je omezena na dobu 3 let, poté je možné certifikát obnovit.

Pro oblast lékárenství však dosud nebyl žádný kodex chování vydán a jedná se tedy pouze o možný další vývoj na poli ochrany osobních údajů. Stejně tak nebyl dosud akreditován subjekt pro vydávání osvědčení o ochraně osobních údajů.

Co se týče poradní a výkladové činnosti Úřadu, je vhodné zmínit, že došlo ze strany Úřadu ke změně v posuzování systémů využívajících biometrické údaje. Úřad v návaznosti na obecné nařízení upozorňuje, že nelze do budoucna již vycházet z jeho stanoviska č. 1/2017 – Biometrická identifikace nebo autentizace zaměstnanců, ale bude vydáno stanovisko nové, aktuální. Pokud tedy nyní uvažujete o zavedení některého z biometrických docházkových či přístupových systémů, doporučujeme s jeho implementací vyčkat na nové stanovisko Úřadu.

Poslední diskutovanou oblastí je možnost uplatnění výjimky podle čl. 30 odst. 5 obecného nařízení, které pro určité správce, konkrétně pro podnik nebo organizaci zaměstnávající méně než 250 osob, formálně zakotvuje výjimku z povinnosti vést tzv. záznamy o činnostech zpracování, pokud není naplněn některý z předpokladů vyjmenovaných v daném článku obecného nařízení. Problematickým se z pohledu výkladu jeví především předpoklad, že správce nemusí vést záznamy o činnostech zpracování za předpokladu, že jím prováděné zpracování osobních údajů je příležitostné. Odborná literatura a především sám Úřad se vyjadřují v tom smyslu, že každé zpracování není příležitostné, a proto je uvedená výjimka v praxi neaplikovatelná. S odkazem na uvedený názor Úřadu tedy nelze než doporučit, aby každý správce, bez ohledu na rozsah své činnosti, vedl záznamy o činnostech zpracování, a to nejen ve vztahu ke svým zákazníkům, ale i zaměstnancům.

Podáváme Vám tuto zprávu a jsme s pozdravem

JUDr. Jakub Havlíček, advokát
HAVLÍČEK & PARTNERS,
advokátní kancelář, s.r.o.

30. července 2019 13:52
CN=JUDr. Jakub Havlíček
OU=2, serialNumber=77 11 131
ISSUER CN=PostSignum Qualified CA 3