

Vážené kolegyně, vážení kolegové,

dovolte nám Vám poskytnout základní informace k obecnému nařízení o ochraně osobních údajů (GDPR), které jsou v poslední době velkým tématem ve sdělovacích prostředcích s ohledem na různé kauzy zejména nadnárodních společností, kdy došlo k únikům osobních údajů nebo s nimi bylo neoprávněně obchodováno, a to je i patrně důvodem širší společné regulace Evropské unie, která tak dopadá přímo i na nás. Hlavním deklarovaným smyslem GDPR je vrátit kontrolu nad osobními údaji zpět subjektům údajů.

GDPR – OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Dne 4. května 2016 bylo v Úředním věstníku EU zveřejněno **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/ES („GDPR“)**. Jedná se o přímo závazné nařízení Evropské unie, které se automaticky stává součástí právního řádu ČR. **Účinnost nastává dnem 25. května 2018**. Současný zákon o ochraně osobních údajů bude zrušen a nahrazen tzv. adaptačním zákonem, jenž upraví otázky, které GDPR ponechává na jednotlivých státech.

Přestože se jedná o legislativu Evropské unie, **GDPR bude mít celosvětový dopad, může se totiž uplatnit i na zpracování prováděné správci či zpracovateli usazenými mimo EU**.

Nařízení GDPR obecně **posiluje práva subjektů** údajů a přináší některá práva nová, například právo být zapomenut: pokud o to subjekt údajů požádá, je správce povinen vymazat jeho osobní údaje (i když zrovna toto právo se v případě zpracování údajů pro účely poskytování zdravotních služeb neuplatní, protože uchování zdravotnické dokumentace po určitou dobu je dáno ze zákona).

Dle GDPR patří údaje o zdravotním stavu mezi zvláštní kategorie osobních údajů. GDPR již neuznává termínu citlivý údaj.

GDPR ukládá zejména správcům (ale i zpracovatelům) velké množství nových povinností, jako například jmenovat tzv. pověřence pro ochranu osobních údajů (týká se však jen některých správců a zpracovatelů), vést záznamy o zpracování, zavést vhodná technická a organizační opatření k ochraně osobních údajů, hlásit případy porušení zabezpečení osobních údajů apod.

Důležité je zmínit, že **GDPR je založeno na zásadě odpovědnosti, která znamená, že nestačí „pouze“ nařízení dodržovat, ale že jeho dodržování je zapotřebí aktivně prokázat a zajistit**. Proto nařízení ukládá povinnost vytvoření řady písemných dokumentů, standardních operačních postupů a katalogů, které musíme všichni (nejen poskytovatelé zdravotních služeb), kteří nakládáme s osobními údaji, připravit, uchovávat a aktualizovat a také o nich zaškolit své zaměstnance.

Nařízení stanoví poměrně vysoké sankce za porušení povinností, které mohou dosáhnout až 20.000.000 EUR nebo u velkých společností výše 4 % celosvětového ročního obrátu, ale dle našeho názoru by se zde měla uplatnit zásada přiměřenosti a sankce ve vztahu k poskytovatelům zdravotních služeb (zejména ambulantním specialistům) by se měly pohybovat výrazně níže.

Je nutné si také uvědomit, že v případě ambulantních specialistů, stejně tak i dalších poskytovatelů zdravotních služeb, se **nejedná jen o otázku dat pacientů. Jako podnikatelé nakládáme s mnoha dalšími osobními údaji** (např. jako zaměstnavatelé s údaji svých zaměstnanců), i při zpracování těchto dat je nutné jednat v souladu s novými pravidly GDPR.

ZÁVĚR

Tím, že je nařízení obecné a hlavně nové, se můžete setkat s různým výkladem určitých povinností a jejich naplnění. Nicméně i to je celkem obvyklé, sami jsme na Úřad na ochranu osobních údajů a Ministerstvo zdravotnictví několik dotazů vznesli, jelikož obecnost nařízení otázky přímo vyvolává. Praxí a hledáním cest k naplnění tohoto právního předpisu se jeho výklad bude, doufejme, postupně zpřesňovat.

Jsmo připraveni Vám být v GDPR a jeho implementaci nápomocni, ať už prostřednictvím workshopů, které v současné době připravujeme (např. 7. 4. v Praze), nebo přímo v rámci Vašich konkrétních otázek.

S úctou a pozdravem
**Gastroenterologická asociace
České republiky, z.s.**