

## Resort zdravotnictví je na GDPR připraven, nové požadavky zdravotníky příliš nezatíží

Od 25. května vstupuje v účinnost evropské nařízení o ochraně osobních údajů neboli GDPR. Hlavním účelem GDPR, stejně jako doposud platného zákona o ochraně osobních údajů, je ochrana soukromí člověka. Resort zdravotnictví je na nové požadavky připraven. *„Připravili jsme metodiku pro ambulantní poskytovatele zdravotní péče a pro lůžková zařízení, která jim pomůže přizpůsobit se novým požadavkům, jež na ně GDPR klade. Ačkoliv se oproti současnému stavu nejedná o velkou změnu, je potřeba se naučit tímto nařízením přísně řídit. V dnešní moderní době, která klade čím dál větší důraz na ochranu osobních údajů jednotlivce, jde o naprostou nezbytnost,“* vysvětlil náměstek ministra zdravotnictví pro legislativu a právo Radek Polícar s tím, že zdravotníky změny příliš nezatíží a pacienti je téměř nezaznamenají.

Ve zdravotnictví je většina procesů zpracování osobních údajů stanovena zákonem, netřeba tedy pro zpracování osobních údajů souhlas subjektu údajů. Ten bude potřeba typicky jen u určitých „nadstavbových“ aktivit, jako je např. výzkum. **Nehrozí tedy, že by se nově vyžadovaly souhlasy pacientů** (čili další „papíry“) v těch případech, ve kterých dosud vyžadovány nebyly. GDPR zavádí nově **povinnost** u středně velkých a velkých poskytovatelů zdravotních služeb **ustanovit pověřence pro ochranu osobních údajů** (toto nebude třeba u malých ambulancí), který bude jakýmsi poradcem a auditorem pro oblast ochrany osobních údajů.

Ministerstvo zdravotnictví a Ústav zdravotnických informací a statistiky spolu s odborníky na danou problematiku a s Úřadem pro ochranu osobních údajů připravili **implementační metodické materiály k praktickým aspektům zavedení GDPR v klinické praxi**:

1. Metodika pro lůžková zařízení (<https://www.uzis.cz/metodika-implementace-gdpr#gdpr>)
2. Metodika pro ambulantní poskytovatele ([https://www.uzis.cz/metodika-implementace-gdpr#amlulant\\_gdpr](https://www.uzis.cz/metodika-implementace-gdpr#amlulant_gdpr))

Metodiky jsou distribuovány v omezeném nákladu jako tištěné brožury a zejména pak v elektronické verzi. S poskytovateli zdravotních služeb **navíc probíhají pravidelná setkání, kde jsou diskutovány různé aspekty a problémy implementace GDPR**. Odborníci z MZ ČR a ÚZIS ČR také od listopadu 2017 tuto problematiku přednášejí na odborných akcích a konferencích.

## VÝBĚR DOPORUČENÍ PRO AMBULANTNÍ POSKYTOVATELE ZDRAVOTNÍCH SLUŽEB

Níže uvedený výčet představuje základní minimum kroků pro zajištění ochrany osobních údajů, které by měly být postačující pro běžnou ambulantní praxi a které neznamenaají žádný zásadní zásah do její běžné činnosti.

- 1) **Katalog osobních údajů**, tj. tabulka, kde si vypíšete, jaké údaje jsou kde zpracovávány a vedeny a proč (prostý přehled) – důležitý je účel a rozsah vedených údajů. Je to v podstatě INVENTURA, jejímž výsledkem může být i to, že ambulance vede údaje, které vést nemusí nebo by je neměla mít v daném rozsahu.
- 2) **Katalog operací zpracování osobních údajů** – opět v podstatě tabulka, jednoduchý přehled shrnující operace, které se s údaji v provozu dělají, může být spojena i s katalogem osobních údajů, může být jejím pokračováním.
- 3) Jasně **zavedená agenda přístupů** k osobním údajům – tedy jasně pojmenované osoby, které mají přístup a k čemu, nejlépe formou jakési vnitřní směrnice, je třeba nezapomenout na úplně obyčejná opatření, ke kterým patří například i zamykání ordinací či natočení monitoru tak, aby je nebylo možné sledovat třetími osobami, resp. nepovolanými osobami.
- 4) Doklad o tom, že osoby, které pracují s osobními údaji a mají k nim přístup, byly **řádně proškoleny**, resp. poučeny, co dělat mají a co nesmí. Ideální je nechat si toto poučení podepsat – zejména tam, kde je takových osob více a může hrozit selhání lidského faktoru.
- 5) **Analýza souladu** – navazuje na body 1) až 4) – poskytovatel by si měl podle vzoru ověřit, že má systém nastavený tak, aby byl ve shodě s GDPR (posouzení vlivu). Jde o velmi jednoduchý dokument, zejména u malých pracovišť, postačí i forma jednoduché tabulky. Je však povinností poskytovatele ZS ji mít.
- 6) **Analýza a hodnocení rizik** – dokument, který může navázat na Analýzu souladu, v podstatě dle jednoduchého vzoru pojmenovává slabá místa, kde může dojít k problémům se zpracováním osobních údajů, a k tomu přijatá opatření, která riziko minimalizují. MV ČR sice analýzu rizik u malých provozů striktně nevyžaduje, nejedná se ale o nic složitého a její provedení je možné doporučit. Jde o to se zamyslet nad tím, jestli nemůže dojít k úniku osobních údajů ve vztahu k nepovolaným osobám, jaké by to případně mohlo mít následky a co jsme udělali, abychom riziko eliminovali. Přitom nezapomenout na úplně obyčejná opatření – viz výše bod 3).
- 7) **Technická a organizační opatření** = viz bod 6, dokumenty lze propojit. Jaká opatření jsou přijata, aby nedošlo k nesprávné manipulaci s osobními údaji.
- 8) **Řádně podepsaná smlouva s IT dodavateli** – smlouva vymezující jejich povinnosti v zabezpečení IT systémů a v ochraně přístupů, měla by obsahovat kapitolu o zpracování



osobních údajů. Stačí i dodatek, je-li uzavřena na delší období. Tento bod je podstatný, neboť smlouva jasně vymezující povinnosti v podstatě chrání poskytovatele zdravotních služeb, který samozřejmě nemůže kontrolovat a zabezpečovat technické parametry dodávaného informačního systému.

- 9) **Připravená informace pro pacienty** – připravený jasný dokument (přibližně jedna stránka A4), který pacienta informuje, že dané pracoviště řádně postupuje a osobní data chrání – informace bude obsahovat stručnou sumarizaci výše uvedených dokumentů zejména s odkazem, že osobní údaje jsou zpracovávány na základě zákona.
- 10) **Připravený informovaný souhlas** – netýká se běžného provozu a poskytování péče; je ale nezbytný v případě zapojení do výzkumu, u klinických studií či jakýchkoli aktivit a zpracování dat, které nesouvisí s vlastním poskytováním péče.

**K plnění a kontrolování výše uvedených kroků je možné jmenovat zaměstnance, který bude určen jako „pověřenec pro ochranu osobních údajů“. U malých ambulancí je toto zcela nepovinné.**

*Ing. Gabriela Štěpanyová*  
*vedoucí tiskového oddělení, tisková mluvčí*  
[tisk@mzcr.cz](mailto:tisk@mzcr.cz)

