GDPR - Obecné nařízení pro ochranu osobních údajů

Společnost MEDAX Systems s.r.o. jako dodavatel ambulantního programu SmartMEDIX pečlivě sleduje legislativu související se zavedením GDPR. Komise EU pro GDPR vytvořila právní prostor jednotlivým zemím provést závazné místní úpravy GDPR. Každé rezortní ministerstvo (v daném případě Ministerstvo zdravotnictví) má do začátku platnosti GDPR možnost legislativou závazně upřesnit a upravit směrnici GDPR ve svém rezortu v daném státě. Z těchto důvodů není právní podoba GDPR pro ČR definitivní a je očekáváno upřesnění v podobě prováděcí vyhlášky či jiného předpisu.

Klient či pacient vystupuje jako subjekt osobních údajů. Zdravotnické zařízení vystupuje jako správce osobních údajů. Povinnosti z hlediska litery zákona jsou tyto:

1) Uplatnění principu zodpovědnosti a zavedení technicko-organizačních opatření k ochraně osobních údajů.
2) Omezení účelu – osobní údaje smí být shromažďovány pouze pro legitimní účely, zákonně, korektně, transparentně a v minimální nutné míře.
3) Posouzení stavu ochrany osobních údajů – audit pověřencem pro ochranu osobních údajů.
4) Předchozí konzultace = souhlas subjektů osobních údajů se zpracováním.
   Souhlas není vyžadován, vyplývá-li zpracování osobních údajů ze zákona nebo se jedná o ohrožení zdraví či života.
5) Jsou nově definována práva subjektu vůči správci, jedná se zejména o právo na výmaz (archivaci).
6) Ohlašovací povinnost porušení zabezpečení ochrany osobních údajů Úřadu pro ochranu osobních údajů.
7) Oznamovací povinnost porušení zabezpečení ochrany osobních údajů subjektu.

Implementačně má GDPR několik rovin:

1) Organizační opatření – výběr zaměstnanců s přístupem k informačnímu systému, proškolení uživatelů, doplnění pracovních smluv atd.
2) Technická opatření – zabezpečení fyzického přístupu k IT technice, zajištění politiky přístupových práv, hesel, zabezpečení přenosů dat, využívání mobilních počítačů atp.
3) Ošetření smluvních vztahů se subjekty přistupujícími k systému např. v rámci podpory, IT služeb apod. Podpora vystupuje jako zpracovatel osobních údajů.
4) Institut pověřence pro ochranu osobních údajů – jedná se o zaměstnance nebo externího poskytovatele na základě smlouvy, který dohlíží na dodržování GDPR. Poskytuje rady a spolupracuje s vedením firmy a s dozorovým úřadem.
   Z dostupných zdrojů se jeví, že pro menší zařízení (do 10000 záznamů nebo do 250 zaměstnanců) postačí jednorázový audit zabezpečení osobních údajů. Pro větší zařízení je vyžadován audit každý rok.

Hlavní váha na zavedení GDPR do praxe bude ležet na správci osobních údajů, tj. na daném zdravotnickém zařízení. Pracovníci společnosti MEDAX Systems s.r.o. jsou připraveni poskytnout podporu a součinnost při implementaci GDPR v záležitostech souvisejících s programem SmartMEDIX. SmartMEDIX bude splňovat náležitosti normy GDPR. Implementace GDPR do systému přinese zpřísnění režimu práce – vynucení silnějších hesel, automatické odhlašování při nečinnosti, možnost přidělení určitého pacienta jen vybranému personálu, sledování přístupů a další.

Výše uvedený text byl sestaven na základě analýz dostupných zdrojů a společnost MEDAX Systems s.r.o. nenese žádnou zodpovědnost za případnou vadu či nepřesnost informací.

MEDAX Systems s.r.o., Oběžná 2075/11, 709 00 Ostrava
Tel.: +420 733 398 440, e-mail: podpora@medax.cz