GDPR - Obecné nařízení pro ochranu osobních údajů

Obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR) je Nařízení Evropského parlamentu a Rady (EU) 2016/679, jehož účelem je výrazně zvýšit ochranu fyzických osob v souvislosti se zpracováním jejich osobních údajů. Bylo přijato v dubnu 2016, v účinnost vstoupí od 25. května 2018. GDPR představuje právní rámec ochrany osobních údajů v evropském prostoru s cílem hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich daty včetně osobních údajů. Nařízení se týká všech firem, institucí, jednotlivců a online služeb, které zpracovávají data uživatelů.

Společnost **Sefima s.r.o.** jako dodavatel „MSS Medixen“ sleduje velmi podrobně legislativu související se zavedením GDPR.

Pacient nebo klient je brán jako subjekt osobních údajů. Zdravotnické zařízení vystupuje jako správce osobních údajů.

Povinnosti správce z hlediska litery zákona jsou následující:

1. Uplatnění principu zodpovědnosti a zavedení technicko-organizačních opatření k ochraně osobních údajů.
2. Osobní údaje smí být shromažďovány pouze pro legitimní účely, zákonně, korektně, transparentně a v minimální nutné míře.
3. Je zavedena instituce „pověřenec pro ochranu osobních údajů“ – který posuzuje stav ochrany osobních údajů
4. Souhlas není vyžadován, vyplývá-li zpracování osobních údajů ze zákona nebo se jedná o ohrožení zdraví či života.
5. Jsou definována rozšiřující práva subjektu vůči správci (právo na výmaz dat, právo na znalost rozsahu osobních dat, atd.).
6. Oznamovací povinnost porušení zabezpečení ochrany osobních údajů subjektu.
7. Ohlašovací povinnost porušení zabezpečení ochrany osobních údajů Úřadu pro ochranu osobních údajů.

Implementačně má GDPR několik rovin:

1. Organizační opatření – minimalizace práv zaměstnanců s přístupem k citlivým údajům, doplnění pracovních smluv, kodex uživatele, minimalizace přístupových práv uživatelů , proškolení uživatelů
2. Technická opatření – zabezpečení fyzického přístupu k IT technice, zajištění politiky přístupových práv, hesel, zabezpečení přenosů dat, využívání přenosných počítačů atd.
3. Ošetření smluvních vztahů s dodavateli služeb přistupujícími k systému v rámci podpory, IT služeb apod.
4. Institut pověřence pro ochranu osobních údajů – jedná se o externího poskytovatele na základě smlouvy, který dohlíží na dodržování GDPR.
   Poskytuje rady a spolupracuje s vedením firmy a s dozorovým úřadem. Audit je vyžadován každý rok.

Hlavní váha na zavedení GDPR do praxe bude ležet na správci osobních údajů, tj. na daném zdravotnickém zařízení.

MSS Medixen splňuje náležitosti normy GDPR.

Obecné náležitosti

- Logování přihlášení/odhlášení
- Logování spuštěných výstupů
- Vynucení silnějších hesel
- Automatické odhlašování při nečinnosti

Specifické náležitosti

- Rozdělení uživatelů na ty, kteří mají přístup k osobním datům a na ty, kteří nemají
- Sledování, kterých rodných čísel se výstupy týkaly, rozděleno na hromadné výstupy a individuální práce s konkrétním rodným číslem
- Zobrazení kontaktních údajů jen pověřeným osobám
- Vyžádaná archivace při odebrání souhlasu
- Anonymizace dat po uplynutí stanovené doby pro úplnou evidenci dat
- Evidence souhlasů a odvolání souhlasů pacientů / klientů
- Vyžádaná archivace při odebrání souhlasu
- a další