

GDPR a jeho dopad na informační systémy od Petr Zajíc software

Jak možná víte, 25. 5. 2018 vstoupí v platnost evropská směrnice „Obecné nařízení o ochraně osobních údajů“, anglicky „General Data Protection Regulation“, známé také pod zkratkou GDPR.

Směrnice se týká všech, kdo zpracovávají osobní data uživatelů, tedy i poskytovatelů sociálních služeb. Poskytovatelé typicky zpracovávají osobní data klientů - uživatelů, pracovníků, případně dalších osob.

Obecným záměrem této směrnice je dát evropským občanům větší kontrolu nad tím, co se děje s jejich osobními daty a v určitých případech jim dává práva požadovat, aby jim zpracovatel tato data vydal, případně aby je ze svých informačních systémů odstranil.

Směrnice tak de facto nahrazuje současně platnou právní úpravu, zejména zákon 101/2000 Sb., o ochraně osobních údajů a podstatným způsobem rozšiřuje práva lidí, kterým údaje patří a povinnosti těch, kdo údaje zpracovávají.

Za nesplnění povinností při práci s osobními daty budou nově hrozit astronomické pokuty, které by byly pro většinu poskytovatelů sociálních služeb likvidační. Maximální výše pokut pro záměrnost je 20000000 EUR nebo 4% z celkového ročního obrátu společnosti (platí vyšší z obou možností).

Co to znamená pro nás?

Poskytovatel sociálních služeb se musí ujistit, že procesy ve firmě, při nichž se zachází s osobními údaji odpovídají této Směrnici. Jedná se o všechny procesy počínaje prací s osobními údaji vytištěnými někde na papíře a konče prací v informačních systémech.

Dodavatel informačních systémů (tedy v tomto případě firma Petr Zajíc software) musí informační systémy přepracovat takovým způsobem, aby umožňovaly splňovat požadavky Směrnice, jako je například právo klienta být zapomenut.

Poskytovatel sociálních služeb i dodavatel informačních systémů musejí v tomto procesu úzce spolupracovat. Pokud byste potřebovali další informace ke GDPR, nebo pokud byste uvítali specializované školení na toto téma, dejte nám vědět, rádi přijedeme.

GDPR, informační systémy a často kladené otázky

Jaké konkrétní funkce musí nově informační systémy splňovat, aby byly kompatibilní s GDPR?

Stručně řečeno jde hlavně o tři věci. Informační systémy musejí nově od 25. 5. 2018 „umět“:

- 1) V odůvodněných případech anonymizovat osobní údaje tak, aby nebylo možné zpětně spojit zpracovávané údaje s konkrétní osobou.
- 2) V odůvodněných případech pseudonymizovat osobní údaje tím, že zpracování a klíče umožňující spojit údaje s konkrétní osobou jsou ukládány odděleně.
- 3) Exportovat osobní údaje ve strojově čitelném formátu a poskytnout je občanovi, pokud si o to občan požádá (neboli jakási přenositelnost).

To vypadá na značný zásah do informačních systémů. Kdo jejich vývoj, úpravy a implementaci zaplatí?

Především je nutné zopakovat, že Směrnice se týká všech zpracovatelů osobních dat plošně, tedy v případě poskytovatelů sociálních služeb organizací velkých, stejně jako malých.

Dále, implementace změn si vyžádá v každém z našich informačních systémů tisíce hodin změn a bude stát stovky tisíc korun, spíše milióny.

A konečně, je nám jasné, že finanční situace většiny poskytovatelů sociálních služeb je – mírně řečeno – napjatá.

Po úvaze jsme se tedy rozhodli nepožadovat od poskytovatelů sociálních služeb žádné jednorázové finance na úpravy informačních systémů a náklady pokrýt z roční uživatelské podpory.

Smlouvy, které máme s poskytovateli uzavřeny, nás opravňují roční částku podpory navýšit až o 10%. To nyní využijeme a sazbu roční podpory zvýšíme z původních 4120,- Kč na nových 4530,- Kč.

S trochou nadsázky se tak dá říci, že implementace této Směrnice Vás vyjde na pouhých 410,- Kč.