Identity management a GDPR

Evropské nařízení GDPR ovlivní mnoho oblastí našeho života. Systémy pro správu uživatelských účtů nebudou výjimkou.

ING. MARTIN ŠLANCAR, MBA

Slyšel o něm snad již každý

O GDPR se mluví stále častěji, jak se přibližuje datum počátku platnosti 25. května 2018. Jde o evropské nařízení č. 679/2016, jehož název je ovšem natolik dlouhý, že se pro ně vžila anglická zkratka GDPR, která znamená General Data Protection Regulation.

Tento legislativní předpis sjednocuje pravidla ochrany osobních údajů. Protože jde o evropské nařízení, musejí se jím povinně řídit všechny členské státy EU. Oblast působnosti GDPR je však ve skutečnosti mnohem širší, protože se vztahuje na všechny subjekty, které zpracovávají osobní údaje občanů EU. Nařízením GDPR tedy mohou být „zasaženy" i firmy a organizace mající sídlo mimo EU.

Patrně největším strašákem GDPR je nastavená výše pokut za nedodržování tohoto legislativního předpisu. Postihy mohou být až do výše 20 milionů eur, či do výše 4 % celosvětového obratu firmy podle toho, která hodnota je vyšší.

Jak GDPR ovlivní systémy IDM?

Identita jednoznačně určuje fyzickou osobu, uživatele informačních systémů. V identitě (uživatelském účtu) bývá obvykle uloženo jméno, příjmení a e-mailová adresa uživatele a volitelně další identifikační údaje. Identita tedy rozhodně obsahuje osobní údaje a systémy IDM zpracovávají osobní údaje podle GDPR.

Až tedy budete dělat inventuru zpracovávaných osobních údajů ve vaší firmě, nezaměřujte se pouze na zákaznické databáze, CRM systémy a dodavatele. Svoji pozornost směřujte také k IDM systému, který obsahuje identity vašich zaměstnanců, případně i externích spolupracovníků.

Budete muset sestavit seznam osobních údajů zpracovávaných v IDM, určit všechny účely zpracování osobních údajů a zanalyzovat, jestli dané zpracování podléhá udělení souhlasu subjektem údajů (platí pro komerční firmy), nebo zda vyplývá ze zákona (to platí v případě státních institucí).

Systém IDM bude jedním z klíčových systémů v organizaci, na který budou muset být uplatněna bezpečnostní opatření za účelem zajištění ochrany zpracovávaných osobních údajů. Rovněž budou muset být v organizaci zavedeny nové procesy, pomocí kterých bude firma schopna naplňovat práva subjektů údajů podle GDPR.

Nové procesy

Subjekt údajů má právo požadovat přístup ke svým osobním datům. Prvním novým procesem tedy bude získání všech osobních údajů daného uživatele z IDM a jejich předání uživateli. Jednou z funkcí IDM je často reporting. Není tedy problém vytvořit speciální report, který bude obsahovat požadované osobní údaje uživatele v přehledné struktuře.

Subjekt údajů má dále právo na opravu svých osobních údajů. Vyřízení takové žádosti bude velmi jednoduché, neboť systémy IDM mají administrační aplikace pro správu uživatelských účtů. Pokud je však účet synchronizován z nějakého autoritativního zdroje, je potřeba změnu učinit tam. Opravené údaje se posléze přenesou do IDM.

Dalším poněkud kontroverzním právem je právo „být zapomenut". Subjekt údajů může požadovat smazání svých osobních dat. To může být v případě IDM systému obtížně uskutečnitelné, protože se často uživatelský účet neodstraňuje, ale pouze zablokuje, aby bylo možné zpětně dohledat aktivitu uživatele v informačních systémech i po několika měsících. Navíc samotné identitní atributy, které nesou osobní údaje, bývají často povinné, a nelze je tedy z identity jednoduše odstranit.

Subjekt údajů může také vznést požadavek na omezení zpracování osobních údajů. Osobní údaje mohou být v IDM systému uloženy, ale nesmějí být s nimi činěny žádné operace (zde typicky synchronizace účtu do aplikací integrovaných s IDM). Toto by mohlo být splněno již zmíněným zablokováním účtu. Je ale potřeba zajistit, aby se informace o omezení zpracování osobních údajů přenesla také do integrovaných aplikací a aby tyto aplikace tento příznak respektovaly.

Subjekt údajů může vznést námitku proti zpracování svých osobních údajů. Správce osobních údajů pak musí posoudit oprávněnost této námitky a buď ji zamítnout s uvedením důvodu, nebo ji uznat a ukončit zpracování osobních údajů jejich smazáním.

GDPR také definuje právo na přenositelnost údajů. Správce osobních údajů by měl být schopen subjektu údajů předat zpracovávaná osobní data ve strojově čitelném formátu, aby je uživatel mohl předat dalšímu správci. Tento požadavek může být splněn pomocí exportních nástrojů systémů IDM. Pokud se k osobním údajům přistupuje standardním protokolem (např. LDAP, SQL), lze použít i nástroje třetích stran nebo si připravit vlastní.

Subjekt údajů se může rozhodnout, že nechce být předmětem automatizovaného zpracování osobních dat (tzv. profilování). Pokud systém IDM takovou aktivitu činí, musí být ukončena. Toto právo se ale bude patrně týkat spíše systémů zaměřených na marketing.

Subjekt údajů může také odvolat souhlas se zpracováním osobních údajů. Toto se samozřejmě neuplatní v případě, že osobní údaje jsou zpracovávány ze zákona, kdy udělení souhlasu není potřeba. V případě odvolání souhlasu by správce měl ukončit zpracování osobních údajů daného žadatele, což prakticky může znamenat jejich smazání ze systému IDM.

Je vidět, že GDPR zavádí pro správce osobních údajů mnoho povinností, což povede ke zvýšení jejich nákladů. Nařízení ale dovoluje správci osobních údajů požadovat přiměřený poplatek za vyřízení příslušné žádosti podané subjektem údajů.

Ochrana osobních údajů v systémech IDM

Z pohledu zabezpečení osobních údajů GDPR mluví např. o důvěrnosti, integritě a dostupnosti informačních systémů, čímž fakticky požaduje nasazení systému řízení bezpečnosti informací podle ISO 27001.

GDPR dále konkrétně doporučuje osobní údaje šifrovat či udělat jejich pseudonymizaci. Některá řešení IDM mají šifrování uložených dat zabudováno přímo v sobě. U ostatních není problém šifrovat celé diskové oddíly.

Pseudonymizace je zjednodušeně řečeno o zavedení bezvýznamových identifikátorů, z nichž nelze identifikovat příslušnou osobu bez použití dodatečných informací. Například český e-government by měl pro identifikaci fyzických osob využívat identifikátory AIFO ze základních registrů.

Konečná odpověď?

A co takhle se zcela zbavit osobních údajů! V současných tradičních řešeních je to něco nemyslitelného. Začínají se však již objevovat distribuované IDM systémy, kde osobní údaje nejsou uloženy v jedné centrální databázi.

Autor je business analytikem ve firmě NEWPS.CZ s.r.o.