# Příště nezaspat

Jiří Slíva & DSM

*„Z PLR do MLR jel jsem přes ČSSR...“ zpíval od roku 1980 Ivan Mládek. A zkratek neubývá. V tomto čísle DSM věnujeme zvláštní pozornost dvěma nařízením EP (Evropského parlamentu) a Rady (EU) – eIDAS[1] a GDPR[2]. Zatímco nařízení eIDAS již vstoupilo v platnost, na přípravu na nařízení GDPR máme dva roky.*

*O smysluplnosti eIDAS se všeobecně nepochybuje, žádná revoluce to není, spíše je opožděna naše (a nejen naše) legislativa. Na implementaci nařízení není zatím státní správa připravena, není zpracován harmonogram, vykalkulovány náklady, sestaven poradní tým specialistů... Soukromý sektor netuší, jak a kdy bude do implementace nařízení zapojen. Deset let máme úspěšné datové schránky, ale ministerští úředníci dosud stále nevědí, zda zůstanou národní záležitostí anebo budou zahrnuty pod eIDAS.*

*Máme informační systém základních registrů, v němž již dávno mohl být předem upraven registr práv a povinností. Stávající čip v občance nám bude do její výměny k ničemu; obdržené peníze erár nevrací. Bezplatná výměna občanky za tu s novým čipem alespoň mě osobně neuspokojí, v té době už budu potřebovat pouze seniorpas a hůl.*

*Nařízení GDPR sice vstoupí v platnost až za dva roky, ale mám obavu, že to s implementací tohoto nařízení dopadne stejně. Už jenom sehnat kvalifikovaného správce osobních údajů bude problém a outsourcing této činnosti má svá rizika i náklady.*

*Především musí být správce schopen oddělit rizika týkající se osob od rizik společnosti. To bude vyžadovat vysokou úroveň schopnosti data klasifikovat, a to zejména v nestrukturovaných formátech v dokumentech, prezentacích a tabulkách. Jinak by ale nebylo možné uživateli zajistit realizaci jeho „práva na vymazání dat“.*

*Z požadavku na „omezení uchovávání údajů“ vyplývá nezbytnost vedení informací o účelu shromáždění osobních údajů, tj. potřeba uložení jistého kvanta metadat. Osobní údaje pomocí těchto metadat mohou být pravidelně přezkoumávány s cílem zjistit, zda je nezbytné tyto údaje uchovávat i v budoucnosti.*

*Společnosti budou muset věnovat více pozornosti správě dat, protože osobní data bude třeba sledovat po celý jejich životní cyklus. Mezi povinnosti správce bude navíc patřit „posouzení dopadu na ochranu osobních údajů“ ještě před vlastním zahájením zpracování dat. V případě nestrukturovaných dat bude třeba sledovat, kdo k nim má přístup (např. z hlediska rolí) a kdo ten přístup povoluje. Vyplývá z toho i nezbytnost aktualizovat bezpečnostní politiky, zahrnout testování osobních údajů do penetračních testů, zamyslet se nad dodavateli a nad zpracováním v cloudech atd. Nedovedu si představit, že to vše stávající ÚOOÚ stihne systematicky kontrolovat – asi bude opět jen řešit stížnosti.*

*Otázkou zůstává, do jaké míry GDPR odráží moderní trendy e-commerce, někteří toto nařízení obviňují z recyklace německého Bundesdatenschutzgesetz s tím, že je nová kvalita pouze v extrémní výši pokut. V tomto čísle máme rozhovor s kompetentním odborníkem ze země, která pro nás z hlediska ochrany dat může představovat „zemi, kde zítra znamená včera“. Úkoly jsou v jedné z jeho odpovědí na mé otázky vyjmenovávány jasně bod po bodu, tak jak se v této zemi vždy metodicky postupuje.*

*Často se diskutuje o tom, zda nejsme různými nařízeními EU přeregulováni. Nařízeními eIDAS a GDPR to určitě nebude. Náš problém je jiný – nezaspat. Jinak můžeme jet s poslední slokou písně Ivana Mládka: RNDr. CSc. z ČVUT dá DKW, SPZ ABT 25-50 do šrotu.*

[1] Nařízení 910/2014 ze dne 23. července 2014 „o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES“

[2] Nařízení 2016/679 ze dne 27. dubna 2016 „o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES“ (General Data Protection Regulation – GDPR).