pomůže účastníkům Akademie zvládnout expert na právo informačních a nových technologií firmy PRK Partners advokát Jindřich Kalíšek, kterého doplní IT právník Zbyněk Loebl.

Další informace o přednášejících, programech jednotlivých seminářích, registraci a ceníku jsou na webových stránkách Akademie GDPR: http://www.gdprakademie.cz.

(businessinfo.cz, zdroj: Svaz průmyslu a dopravy ČR 2. 6. 2017)

GDPR přinese více práv, povinností i byrokracie

Nová legislativa Evropské unie dokazuje, že termíny informační společnost nebo digitální ekonomika definitivně přešly do reality.

Předpisy jako eIDAS, NIS či GDPR snad i s mírným zpožděním reflektují změny společenských poměrů, jimiž se prolínají informační a komunikační technologie.

Pravidla a zásady sběru, zpracování, uchovávání a výměny osobních údajů obyvatel Evropské unie bude od května 2018 určovat obecné nařízení o ochraně osobních údajů, které je známé pod zkratkou GDPR – General Data Protection Regulation. Evropský parlament jej po více než třech letech vyjednávání schválil 14. dubna 2016. GDPR jakožto nařízení nebude třeba transponovat do národní legislativy členských států. Nahradí směrnici 95/46/ES, která v současnosti upravuje ochranu osobních údajů na unijní úrovni. V případě České republiky rozhodne o nové podobě zákona č. 101/2000 Sb., o ochraně osobních údajů.

Evropská unie se oblasti digitální ekonomiky a zejména zabezpečení jejích transakcí nevěnuje pouze nařízením GDPR. Do května 2018 musí členské státy do svých národních legislativ zapracovat také požadavky směrnice EP a Rady EU č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v unii. Dokument známý pod zkratkou NIS nabyl platnosti vloni v srpnu. V České republice dojde v této souvislosti k novelizaci zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Další změnu do světa elektronických transakcí vneslo nařízení EP a Rady EU č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93 ES. Dokument nabyl účinnosti v červenci 2016. V tuzemské legislativě unijní nařízení vyřadilo ze hry zákon č. 227/2000 Sb., o elektronickém podpisu.

Všeobjímající GDPR

Nařízení GDPR ve zjednodušeném pojetí ošetřuje pět základních oblastí. Jde o zásady zpracování osobních údajů, práva tzv. subjektů údajů (identifikovaných či identifikovatelných fyzických osob), povinnosti správců a zpracovatelů osobních údajů (technická a organizační opatření), dozorovou činnost a spolupráci dozorových orgánů a o právní ochranu, odpovědnost a sankce.

Požadavkům nařízení GDPR se budou muset přizpůsobit všechny subjekty, které zpracovávají osobní údaje spotřebitelů z Evropské unie v souvislosti s nabídkou zboží nebo služeb. Jeho působnost se tedy neomezuje pouze na lokální správce a zpracovatele, ale na všechny společnosti, jež svou nabídkou zboží nebo služeb cílí na unijní spotřebitele. Pozornost by nařízení GDPR měly věnovat všechny subjekty, které aktivně pracují s osobními údaji fyzických osob.

„Nařízení je specifické především v tom, v jaké šíři na správce a zpracovatele osobních údajů dopadá. Bude nutné nejen upravit právní dokumentaci, tj. znění souhlasů, smlouvy o zpracování, vnitřní směrnice a pravidla zpracování osobních údajů apod., ale především kompletně zrevidovat a nově nastavit vnitřní procesy a IT infrastrukturu," říká Viktor Dušek, advokát společnosti KPMG Legal.

Údaje, souhlas, zpracování

Nařízení pracuje s rozšířenou definicí osobních a citlivých údajů. Reflektuje rozvoj informačních a komunikačních technologií, jež starší legislativa nepodchytila. Za osobní údaj GDPR považuje také informaci o poloze uživatele, jeho IP adresu, informace o využívaných zařízeních, metainformace o dřívějším chování při využívání služeb apod.

Rozšířená definice tedy do jisté míry ošetřuje známou problematiku tzv. cookies. Mezi citlivými údaji figurují mimo jiné genetická a biometrická data, údaje o zdravotním stavu nebo o sexuálním životě fyzické osoby.

Subjekty údajů, tj. fyzické osoby, nově získávají mediálně propagované právo být zapomenut. Povinností správce bude bez odkladu vymazat veškeré osobní údaje, které o žadateli vede, pokud neexistuje právní důvod pro jejich držení.

Zpracování osobních údajů, ať už manuální, nebo automatizované, musí být podmíněno zákonným důvodem nebo explicitně daným souhlasem subjektu údajů, tj. samotné fyzické osoby. Ta má právo udělený souhlas kdykoliv odvolat. Obecně platí, že udělení souhlasu musí být svobodné, určité, informované a jednoznačné.

Povinnosti správců a zpracovatelů

Pro správce a zpracovatele, vedle subjektu údajů a dozorového orgánu údajů dvě z hlavních rolí v GDPR, vzniká povinnost zavedení řady technických a organizačních opatření. V obecné rovině jde stále o známou mantru důvěrnosti, integrity a dostupnosti, nově doplněnou o odolnost systémů. Zavedení a schopnost dodržování technických a organizačních opatření, tj. záměrnou ochranu osobních údajů (by design) musí být správce schopen kdykoliv doložit. Stejně tak musí deklarovat dozorovým orgánům, a to již v době záměru či návrhu zpracování osobních údajů, konkrétní účel zpracování a posouzení vlivu na ochranu údajů.

„Vzhledem k tomu, že šetření a posuzování dopadu budou vždy specifické ke konkrétnímu zpracování osobních údajů, předpokládáme v nejbližší době vznik šablon a příruček k rychlejšímu zvládnutí analýzy a přípravy popisu zpracování," dodává k tématu předběžného šetření Petr Žikeš, výkonný ředitel firmy Safetica.

Správci a zpracovatelé osobních údajů musí mimo jiné pravidelně testovat, posuzovat a hodnotit účinnost zavedených opatření. K nim patří na technické úrovni povinnost pseudonymizace, kryptografické ochrany nebo zálohování a obnovení osobních údajů v případě havárie. První uvedený termín popisuje způsob zpracování, resp. úpravy osobních údajů, který zajistí, že je nelze bez dodatečných informací přiřadit konkrétnímu subjektu údajů. Pseudonymizované údaje lze zpracovávat nad rámec původně definovaného účelu.

Na správce a zpracovatele se vztahuje také bezodkladná ohlašovací povinnost pro případ porušení zabezpečení osobních údajů. Zpracovatel má ohlašovací povinnost vůči správci, správce vůči dozorovému orgánu, případně dotčené fyzické osobě. Všechny případy narušení musí být dokumentovány. „Je nutné si uvědomit, že metody zpracování a související rizika se budou neustále vyvíjet, a s tím musí počítat také nástroje a postupy dokumentace," říká Ivan Svoboda, manažer rozvoje obchodu společnosti Anect.

Agendu sběru, zpracování, uchovávání a výměny osobních údajů u správce nebo zpracovatele má podle obligatorních požadavků GDPR, jež se ovšem netýkají každého subjektu, zastřešovat tzv. pověřenec pro ochranu osobních údajů neboli DPO – data protection officer. Jmenovaná osoba se může rekrutovat z interních zaměstnanců dotčených subjektů, případně lze pro tuto roli najmout externího poskytovatele služeb.

Problematiku pověřenců komentuje Viktor Dušek ze společnosti KPMG Legal: „Podle odhadu mezinárodní asociace IAPP bude v rámci Evropské unie potřeba ustanovit přibližně 28 000 pověřenců. Přesnější odhady konkrétně pro Českou republiku nejsou ještě známy, nicméně je zřejmé, že velká část pověřenců bude činná ve veřejném sektoru, kde bude tato funkce bez výjimky povinná."

Nařízení GDPR doprovází také nebývale vysoké náhrady a sankce za jeho porušení. Každý, kdo utrpí újmu, a to i nemajetkovou, v důsledku jeho nedodržení, má právo na náhradu. Za samotné porušení základních zásad hrozí správní pokuta ve výši až 20 milionů eur, případně čtyř procent z celosvětového obratu podniku.

Průvodce přípravou na GDPR

Jak se na účinnost GDPR připravit? V prvé řadě je třeba zdůraznit, že rozhodně nejde o ryzí IT záležitost.

„Příprava na GDPR vyžaduje komplexní přístup k implementaci nařízení a zapojení odborníků s různými specializacemi a zkušenostmi, zejména v oblasti práva, řízení rizik, IT a bezpečnosti. Proces přípravy na GDPR se napříč trhem liší a je do značné míry odvislý od velikosti organizace a míry zpracování osobních údajů," říká Viktor Dušek ze společnosti KPMG Legal.

Konzultační a bezpečnostní firmy i nejrůznější oborové organizace nabízejí vedle asistence vlastních specialistů také kontrolní seznamy, s jejichž pomocí lze podnik, jeho technologie a procesy s požadavky nařízení sladit. V organizační rovině jde především o relevantní nastavení procesů a vyhodnocení jejich souladu s legislativou. O přibližující se účinnosti GDPR by měli být zevrubně zpraveni manažeři s rozhodovací pravomocí. Následně si organizace musí zmapovat, jaká data sbírá, ukládá, spravuje, sdílí a odkud pocházejí.

„Pro tento krok je ideální zrealizovat tzv. datovou inventuru," jak dodává Ivan Svoboda ze společnosti Anect.

V dalším kroku si organizace zkontroluje, jak dokáže plnit požadavky nařízení, jež se vztahují k individuálním právům. Konkrétně jde o schopnost bezodkladného smazání osobních dat a o možnost jejich poskytnutí v elektronické podobě a ve standardním formátu. Současně je třeba aktualizovat procedury, které ke splnění individuálních požadavků subjektů osobních informací vedou.

Právníci organizace by měli nad výsledky informačního auditu zjistit, zda sběr a zpracování osobních údajů vyhovují legislativním požadavkům. Tento krok musí zdokumentovat, neboť účel zpracování spadá mezi povinně prokazované informace. Stejným procesem validace musí projít také postup získávání a zaznamenávání souhlasu subjektů osobních informací

se zpracováním. Specifickou problematiku představují požadavky nařízení GDPR na tzv. záměrnou ochranu osobních dat, resp. data protection by design. Ta do značné míry souvisí s technickými prostředky a jejich nastavením. Záměrná ochrana osobních údajů reprezentuje přístup, který zajišťuje, aby záruky týkající se ochrany údajů byly začleněny do relevantních systémů již v okamžiku jejich vývoje.

Tuto ideu potvrzují i slova Petra Žikeše ze společnosti Safetica: „Mnohem větší důraz bude kladen na bezpečnost už při samotném návrhu a výběru systémů pro zpracování osobních dat. Systémy CRM nebo ERP, ale i docházka, finance, ty všechny budou muset chránit data před útočníky zevnitř i zvenčí."

Tímto způsobem, tj. záměrnou ochranou, lze do jisté míry eliminovat nedostatky a problémy vzniklé či potenciálně vznikající na straně organizačního zajištění. Nutno podotknout, že toto pojetí představuje ideální stav či přístup. „Lze také předpokládat, že IT systémy, které nebudou dostatečně vyhovovat nové regulaci, budou postupně nahrazeny," dodává Martin Hladík ze společnosti KPMG Česká republika?

* * *

Aktuálně v rámci Evropské unie existuje 28 různých zákonů o ochraně osobních údajů. Pokuty v řádech desítek milionů za nesplnění GDPR umožňují každému snadno vyhodnotit důležitost investice do zabezpečení dat.

(Hospodářské noviny 23. 2. 2017)

Fungování veškerých firem v ČR významně ovlivní nové nařízení z dílny EU

Řeč je o tzv. GDPR (The General Data Protection Regulation), které pod názvem Obecné nařízení o ochraně osobních údajů vstoupí plošně v celé EU v platnost 25. 5. 2018. V Česku nahradí současnou právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES. Při nedodržení nových pravidel hrozí všem pokuty v řádu až stovek milionů korun.

Co můžete od nového nařízení čekat a jak nejlépe předejít možným pokutám?

Změny se nevyhnou téměř nikomu

Nové nařízení se dotýká všech podnikatelů či subjektů veřejné správy, kteří zpracovávají jakékoli databáze osobních údajů nejen zákazníků, ale i zaměstnanců, pacientů, hostů a podobně. „Největší nedostatky bývají v oblasti samotného zabezpečení údajů. Právě bezpečnost je přitom hlavním motivem těchto změn a ze strany EU bude jistě nejvíce ověřována," říká Michal Grepl, produktový manažer společnosti Konica Minolta Business Solutions Czech, která se komplexní analýzou zpracování osobních údajů v souladu s GDPR v ČR zabývá.

Na co se konkrétně zaměřit?

Při ověřování správného zpracování osobních údajů je třeba prověřit především zajištění kybernetické bezpečnosti, šifrování dat, nastavení vnitrofiremních procesů, zajištění tzv. pseudonymizace nebo adekvátní zabezpečení tiskového prostředí. „Toto prověření a zejména následné implementace nových potřebných systémů či postupů mohou trvat poměrně dlouhou dobu. Ačkoli nové nařízení vstupuje v platnost zhruba za rok, s auditem by měly minimálně velké firmy začít co nejdříve," upozorňuje M. Grepl.

Vhodné technologie nejsou zdaleka vše

Nesmíte opomenout ani právní náležitosti všech příslušných dokumentů, které osobní údaje obsahují. Soulad s pravidly GDPR je proto nutné ověřit také v rámci smluv, interních směrnic nebo například dokumentových šablon. „Při hledání profesionálního auditora zpracování osobních údajů proto doporučujeme zaměřit se na nabídku komplexních služeb, tedy nejen ověření technologických požadavků, ale také posouzení obsahu dokumentů, " dodává M. Grepl.

Pseudonymizace

Jde o zpracování osobních údajů způsobem, který neumožňuje jejich přiřazení ke konkrétnímu člověku bez použití dodatečných informací. Ty musejí být uchovány odděleně s dostatečnou technickou a organizační ochranou.

(Computerworld 30. 5. 2017)