MANAGEMENT RIZIK MSP VE SHODĚ S GDPR

RISK MANAGEMENT IN SME UNDER GDPR

David Král

Abstrakt: *Příspěvek se zabývá problematikou managementu rizik, konkrétně shodou nastavení procesů s Nařízením Evropského parlamentu a Rady 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 (obecné nařízení o ochraně osobních údajů), známém jako GDPR. Ke zmíněné oblasti je možné využít doporučených postupů, článek analyzuje přístupy nabízené v českém i zahraničním prostředí. Jsou zde prezentovány výsledky průzkumu v segmentu malých a středních podniků, ve kterých byla zkoumána kritéria související s uvedenou oblastí managementu a shody s GDPR. Cílem článku je popsat stav shody s GDPR ve zkoumané oblasti mezi dotazovanými malými a středními podniky a prezentovat doporučení týkající se přístupu k managementu rizik pro tento segment organizací.*

Klíčová slova: *GDPR, management rizik, malé a střední podniky.*

Abstract: *The paper discusses the issue of risk management, specifically the area of compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Several recommended practices and standards can be used for the area. The article analyses approaches given in Czech and foreign environment. The results of the survey in the segment of small and medium sized enterprises are presented, which examined the criteria related to the mentioned area of risk management to GDPR compliance. The aim of the article is to describe the state of compliance to GDPR in the area investigated among the interviewed SMEs and to present recommended practices to the risk management approach for this segment of organizations.*

Keywords: *GDPR, risk management, small and medium sized enterprises.*

JEL klasifikace: *G32, K24.*

1 ÚVOD

Malé a střední podniky (dále jen „MSP“) představují v současné době velmi důležitý segment v českém i mezinárodním obchodním prostředí, jsou silnými hráči při podpoře konkurenceschopnosti a investic. K tomu, aby plnily své cíle, jsou MSP stále více závislé na informačních technologiích a především prostřednictvím těchto nástrojů zpracovávají osobní údaje svých zaměstnanců, klientů a partnerů.

Vzhledem k tomu, že malých a středních podniků je v České republice více než 1,1 milionu[10], toto obrovské množství se následně odráží ve vysokém objemu dat, které MSP zpracovávají. V tomto objemu jsou osobní údaje nejčastěji zastoupenou kategorií dat. Definice osobních údajů obsažená v čl. 2 písm. a) směrnice 95/46/ES zní takto: *„veškeré informace o identifikované nebo identifikovatelné osobě („subjekt údajů“); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity“*.[11] Ze zpracování osobních údajů plynou MSP určité právní závazky. Velmi často musí zastávat funkci správce údajů, např. při zpracování osobních údajů zákazníků nebo zaměstnanců. Někdy mohou také převzít roli zpracovatele údajů, např. při poskytování služeb zákazníkům jménem jiné společnosti. Náročnost zpracování osobních údajů prováděných malým a středním podnikem se může výrazně lišit dle oboru podnikání daného subjektu.

Klíčovou povinností správců a zpracovatelů dat je zajistit bezpečnost osobních údajů. V rámci zásad informační bezpečnosti je nutné zachovat důvěrnost, integritu a dostupnost těchto dat a aplikovat přístup založený na rizicích, tzn. čím je vyšší riziko, tím přísnější opatření musí správce nebo zpracovatel osobních údajů přijmout.[12]

[10] MPO. Zpráva o vývoji malého a středního podnikání a jeho podpoře v roce 2017
[11] Směrnice Evropského parlamentu a Rady 95/46 ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[12] ENISA. Guidelines for SMEs on the security of personal data processing.

Existuje mnoho různých metodik a standardů pro posuzování rizik, jejichž cílem je podpora organizací při hodnocení těchto rizik v souvislosti s jejich podnikáním. V nedávné době vznikly také metodiky pro posuzování rizik, spjatých se zpracováním osobních údajů a přijetí příslušných bezpečnostních opatření.[13][14] Zatímco velké společnosti mají možnost reagovat na tyto metodiky a doporučené postupy a vhodně je implementovat do svých procesů, MSP nemají vždy k dispozici potřebné odborné znalosti a zdroje (lidské i materiální). V mnoha případech je pro malé a střední podniky obtížné pochopit specifičnost rizik spojených se zpracováním osobních údajů, jakož i řídit a zvládat tato rizika podle formální metodiky. Tento stav uvádí mnoho MSP do nejistoty, zda korektně zpracovávají osobní údaje a dodržují právní závazky plynoucí z GDPR.

V dalším textu je popsána problematika managementu rizik při implementaci GDPR v segmentu malých a středních podniků a jsou uvedeny doporučené postupy, které pomohou těmto organizacím zvládat rizika související s GDPR. V příspěvku jsou také prezentovány výsledky kvantitativního výzkumu, který se zabýval zkoumanou oblastí, a to metodou dotazníkového šetření.

2 METODIKA A CÍLE PŘÍSPĚVKU

Dokument je zaměřen na oblast managementu rizik, která vznikla nebo se modifikovala v okamžiku, kdy vstoupila v platnost GDPR. Cílem příspěvku je popsat aktuální stav závažných rizik v prostředí malých a středních podniků v České republice a navrhnout možný přístup k managementu rizik v souvislosti s GDPR pro tento segment subjektů.

Pro zpracování příspěvku byla využita kombinace kvalitativního i kvantitativního výzkumu. Při kvalitativním výzkum a sběru dat byla použita metoda analýzy textu, tj. dostupných zdrojů zabývajících se problematikou GDPR ve spojitosti s managementem rizik. Pro primární výzkum, který byl proveden v roce 2018, byla využita metoda dotazníkového šetření na téma Regulace ochrany osobních údajů v evropském prostoru (GDPR). Šetření realizovali studenti bakalářského studia AKADEMIE STING, o.p.s. v rámci předmětu Eseje, ankety, výzkum.

[13] NEZMAR, L. Praktický průvodce implementací, 1. vyd. Praha: GRADA Publishing, 2018, s.304, ISBN 978-80-271-0668-4.
[14] ŽŮREK, J. Praktický průvodce GDPR, 1. vyd. Praha: Anag, 2017, s. 224, ISBN 978-80-554-097-3

Příspěvek je strukturován následovně. Úvodní část je věnována popisu bezpečnostních závazků, které vstoupily v platnost v oblasti ochrany osobních údajů. Důraz je kladen na přehled bezpečnostních zásad plynoucích z GDPR. Následuje zhodnocení dotazníkového šetření a doporučení pro management rizik v oblasti ochrany osobních údajů pro MSP.

3 BEZPEČNOSTNÍ ZÁVAZKY PLYNOUCÍ Z GDPR

Bezpečnost osobních údajů byla vždy zákonným závazkem pro jejich správce, GDPR nicméně posiluje a zpřísňuje pravidla zacházení s těmito daty, přičemž současně rozšiřuje odpovědnost přímo o zpracovatele osobních údajů.

Je důležité upozornit na skutečnost, že bezpečnost (ve smyslu integrity a důvěrnosti) je stanovena jako jedna ze zásad týkajících se zpracování osobních údajů.[15] Tím se zabezpečení stává jádrem ochrany údajů spolu s ostatními definovanými zásadami, tj. zákonností, korektností a transparentností, účelovým omezením, minimalizací, přesností, omezením uložení a odpovědností.

V souladu s tímto obecným principem je bezpečnost zpracování osobních údajů regulována zejména čl. 32 GDPR, který stanovuje, že:

„S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) *pseudonymizace a šifrování osobních údajů;*
b) *schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;*
c) *schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;*
d) *procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.“*[16]

[15] Nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
[16] Nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Tento článek dále stanovuje, jaká rizika se mají zohledňovat při posuzování vhodné úrovně zabezpečení. Jedná se především o: zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim. Uvádí také, že dodržováním schváleného kodexu chování uvedeného v čl. 40 nebo uplatňováním schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42 lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku. Na závěr je uvedeno, že správce a zpracovatel *"přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu."*[17]

4 ZÁSADY BEZPEČNOSTI OSOBNÍCH ÚDAJŮ PODLE GDPR

Na základě ustanovení uvedených v předchozím textu existuje několik důležitých aspektů, které by měly být zohledněny při implementaci opatření k bezpečnosti osobních údajů v rámci GDPR. Z níže uvedených bodů je patrné, že bezpečnost zpracování není izolovaným závazkem v GDPR, který by byl řešen v jednom konkrétním článku. Naopak, bezpečnost by měla být chápána v rámci celkového přístupu k odpovědnosti k ochraně údajů v GDPR, který je založen na hodnocení rizik a na posouzení dopadů a který by měl být zasazen do celkového kontextu procesů a postupů v konkrétní organizaci. V rámci tohoto přístupu lze bezpečnostní opatření na jedné straně považovat za závazek a na straně druhé jako nástroj pro provádění dalších nutných kroků v oblasti ochrany dat, a to zejména v on-line prostředí.

4.1 Přístup založený na hodnocení rizik

Aplikovaná technická a organizační opatření na ochranu osobních údajů by podle GDPR měla odpovídat významu posuzovaného rizika. GDPR stanovuje zvláštní parametry pro ochranu osobních údajů, které je třeba vzít v úvahu při jejich posuzování, zejména se jedná o povahu, rozsah, kontext a účely zpracování. Tento přístup stanovuje dopad možného narušení osobních údajů jako hlavní aspekt při posuzování rizik a měl by být také chápán ve vztahu

[17] Nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

k požadavku na obecné posuzování dopadů ochrany osobních údajů (podle čl. 35 GDPR). Pojem rizika je v GDPR chápán jako klíčová proměnná pro správce při plnění různých povinností, např. pokud jde o ohlašování a oznamování případů porušení zabezpečení (čl. 33 a 34 GDPR) nebo posuzování dopadů na ochranu osobních údajů po předchozí konzultaci s dozorovým úřadem (čl. 36 GDPR).[18]

4.2 Systém správy informací

Ustanovení GDPR přesahuje pouhé přijetí konkrétních bezpečnostních opatření. Doporučuje zavedení systému řízení bezpečnosti informací pro ochranu důvěrnosti, integrity, dostupnosti a odolnosti osobních údajů. Je důležité zdůraznit, že se nařízení rovnoměrně zabývá všemi aspekty bezpečnosti informací, což zahrnuje procesy pravidelného testování, posuzování a vyhodnocení účinnosti přijatých opatření.

4.3 Ochrana soukromí

I když GDPR neposkytuje přímý odkaz na technologie zvyšující ochranu soukromí, za základní opatření pro bezpečnost osobních údajů považuje zejména pseudonymizaci a šifrování. To ukazuje, že GDPR pohlíží na problematiku soukromí komplexně. Tato oblast je rovněž spojena s ustanoveními GDPR v čl. 25,[19] která kladou důraz na technická opatření na ochranu soukromí (např. pseudonymizace) a která nabádají správce, aby shromažďoval pouze osobní údaje, které jsou nezbytné pro daný účel. Tato ustanovení jsou opět spojena také s rizikem zpracování osobních údajů, což znovu funguje jako výchozí hodnota pro přijetí příslušných opatření.

5 DOTAZNÍKOVÉ ŠETŘENÍ GDPR

Šetření se zúčastnilo celkem 289 malých a středních podniků. Zapojené subjekty byly zařazeny do tohoto segmentu na základě doporučení EU (2003/361/ES ze dne 6. května 2003) a aplikačního výkladu MSP, který zpracovalo Ministerstvo průmyslu a obchodu a Úřad pro ochranu hospodářské soutěže [20].

[18] Nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
[19] Nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
[20] http://www.czechinvest.org/data/files/definice-maleho-a-stredniho-podniku-2-1112.pdf

Tabulka 5.1: Definice malého a středního podnikatele

Kategorie podniku	Počet zaměstnanců	Roční obrat	Bilanční suma roční rozvahy
Mikropodnik	< 10	< 2 mil. EUR	< 2 mil. EUR
Malý podnik	< 50	< 10 mil. EUR	< 10 mil. EUR
Střední podnik	< 250	< 50 mil. EUR	< 43 mil. EUR

Zdroj: http://www.czechinvest.org/definice-msp

Shrnutí výsledků je k dispozici v tabulce 5.2. Dotazníkové šetření bylo zaměřeno na problematiku ochrany osobních údajů (zaměstnanců, zákazníků, partnerů) ve čtyřech vybraných oblastech:

- Osobní bezpečnost
- Bezpečnost přístupových práv
- Bezpečnost dat o zaměstnancích
- Bezpečnost dokumentace

Osobní bezpečnost

Oblast se týká politiky a přístupu k heslům, politiky a manipulaci s osobními údaji při práci s mobilními zařízeními a mimo kancelář. Úroveň zabezpečení mezi sledovanými subjekty je v této oblasti na střední úrovni. Problematickými se jeví především správa hesel a práce s mobilními zařízeními, která bývá riziková v mnoha subjektech. Platí zde pravidlo, že s velikostí podniku se kvalita zabezpečení zvyšuje. Paradoxně to neplatí pro zmíněnou problematiku práce s osobními údaji přes mobilní zařízení, kde nejlepších výsledků dosáhly sledované mikropodniky.

Bezpečnost přístupových práv

Oblast se týká politiky a přístupu ke smluvním dohodám týkajících se mlčenlivosti zaměstnanců a třetích stran, školení zaměstnanců v oblasti ochrany osobních údajů a politiky přístupových práv do elektronických systémů subjektu. V této oblasti byla zjištěna mezi zapojenými subjekty střední až vysoká úroveň zabezpečení. Akceptovatelná úroveň ochrany osobních údajů byla zjištěna při procesu ukončení pracovního poměru a následného odebírání přístupových práv a ztráta přístupu k datům ve všech zařízeních. Úroveň zabezpečení v této oblasti není příliš závislá na velikosti subjektu, střední podniky vykazovaly mírně vyšší kvalitu.

Bezpečnost dat o zaměstnancích

Oblast se týká ochrany, sdílení a likvidace osobních údajů zaměstnanců. Zkoumané subjekty vykazují v této oblasti převážně vysokou úroveň zabezpečení. Jedinou problematickou oblastí je souhlas zaměstnanců s využíváním jejich fotografií a videí pro marketingové účely. Více než polovina oslovených subjektů uvádí, že zaměstnanci nejsou s tímto využitím seznámeni nebo žádáni o souhlas. Úroveň zabezpečení není v této oblasti závislá na velikosti podniku.

Bezpečnost dokumentace

Tato oblast obsahuje problematiku postupů pro tvorbu, uchovávání a likvidaci dokumentů. V této oblasti byla zjištěna střední až vysoká úroveň zabezpečení mezi sledovanými subjekty. Horší situace panuje v problematice existence směrnic pro nakládání s osobními údaji, které by obsahovaly postupy pro řešení práv fyzických osob. Ve všech sledovaných otázkách vykazují nejlepší výsledky podniky střední velikosti.

Tabulka 5.2: Výsledky dotazníkového šetření

Otázka	**Subjekty**	**Odpovědi**		
OSOBNÍ BEZPEČNOST				
		ano - všichni	**ano - někteří**	**ne**
Používají zaměstnanci aplikaci pro správu hesel?	mikropodniky	10 (**21%**)	14 (**30%**)	23 (**49%**)
	malé podniky	33 (**22%**)	71 (**47%**)	47 (**31%**)
	střední podniky	23 (**25%**)	46 (**50%**)	22 (**25%**)
		ano	**ne**	
Má správce IT přístup k heslům zaměstnanců?	mikropodniky	15 (**32%**)	32 (**68%**)	
	malé podniky	64 (**42%**)	87 (**58%**)	
	střední podniky	42 (**46%**)	49 (**54%**)	
		ano	**ne**	
Zadávají zaměstnanci hesla nebo pracují s osobními údaji na nezabezpečených stránkách (např. přes mobilní zařízení nebo z domova)?	mikropodniky	12 (**25%**)	35 (**75%**)	
	malé podniky	58 (**38%**)	93 (**62%**)	
	střední podniky	43 (**47%**)	48 (**53%**)	
		ano	**ne**	
Mohou být tištěné dokumenty s osobními údaji volně přístupné pro cizí osoby (nezamčená místnost, skříň, pracovní stůl)?	mikropodniky	7 (**15%**)	40 (**85%**)	
	malé podniky	27 (**18%**)	124 (**82%**)	

	střední podniky	7 (**8%**)	84 (**92%**)	
		ano	**ne**	
Převáží zaměstnanci dokumenty s osobními údaji (např. hromadnou dopravou)?	mikropodniky	14 (**30%**)	33 (**70%**)	
	malé podniky	30 (**20%**)	121 (**80%**)	
	střední podniky	19 (**20%**)	72 (**80%**)	
		ano	**ne**	
Převáží zaměstnanci dokumenty s osobními údaji domů, kde nejsou dostatečně zabezpečeny?	mikropodniky	10 (**21%**)	37 (**79%**)	
	malé podniky	34 (**22%**)	117 (**78%**)	
	střední podniky	8 (**9%**)	83 (**91%**)	
BEZPEČNOST PŘÍSTUPOVÝCH PRÁV				
		ano - u všech	**ano - u části**	**ne**
Jsou povinnosti zaměstnanců při nakládání s osobními údaji stanoveny samostatně v dohodě o mlčenlivosti?	mikropodniky	21 (**45%**)	16 (**34%**)	10 (**21%**)
	malé podniky	70 (**46%**)	40 (**27%**)	41 (**27%**)
	střední podniky	40 (**44%**)	32 (**35%**)	19 (**21%**)
		ano - u všech	**ano - u části**	**ne**
Jsou povinnosti partnerů (třetích stran) při nakládání s osobními údaji stanoveny samostatně v dohodě o mlčenlivosti?	mikropodniky	26 (**55%**)	15 (**32%**)	6 (**13%**)
	malé podniky	73 (**48%**)	46 (**31%**)	32 (**21%**)
	střední podniky	26 (**29%**)	40 (**44%**)	25 (**27%**)
		ano - všichni	**ano - někteří**	**ne**
Jsou zaměstnanci, kteří pracují s osobními údaji, proškoleni ohledně práce s osobními údaji?	mikropodniky	24 (**51%**)	14 (**30%**)	9 (**19%**)
	malé podniky	70 (**46%**)	56 (**37%**)	25 (**17%**)
	střední podniky	57 (**63%**)	30 (**33%**)	4 (**4%**)
		ano	**ne**	
Jsou při ukončení pracovního poměru zaměstnanci odebrána přístupová práva do elektronických systémů, pokud nějaké měl?	mikropodniky	38 (**81%**)	9 (**19%**)	
	malé podniky	126 (**83%**)	25 (**17%**)	
	střední podniky	87 (**96%**)	4 (**4%**)	
		ano	**ne**	
Je při ukončení pracovního poměru zajištěno, že zaměstnanec vymaže lokální kopie dat ze svých dalších zařízení, pokud je měl?	mikropodniky	36 (**77%**)	11 (**23%**)	
	malé podniky	112 (**74%**)	39 (**26%**)	
	střední podniky	80 (**88%**)	11 (**12%**)	
		ano	**ne**	

Jsou všechny přístupy k systémům pracujícím s osobními údaji vázány na konkrétní osoby, aby bylo dohledatelné, kdy a kdo se kam přihlásil?	mikropodniky	23 (**49%**)	24 (**51%**)	
	malé podniky	97 (**64%**)	54 (**36%**)	
	střední podniky	62 (**68%**)	29 (**32%**)	
BEZPEČNOST DAT O ZAMĚSTNANCÍCH				
		ano	**ano - nesmí odmítnout**	**ne**
Dochází k používání fotografií či videí zaměstnanců pro marketingové účely a mohou to bez jakéhokoliv postihu zaměstnanci odmítnout?	mikropodniky	18 (**38%**)	5 (**11%**)	24 (**51%**)
	malé podniky	42 (**28%**)	21 (**14%**)	88 (**58%**)
	střední podniky	28 (**31%**)	15 (**16%**)	48 (**53%**)
		ano	**ne**	
Mají k osobním složkám zaměstnanců přístup pouze oprávněné osoby (např. účetní, personalista, majitel)?	mikropodniky	42 (**89%**)	5 (**11%**)	
	malé podniky	121 (**80%**)	30 (**20%**)	
	střední podniky	76 (**84%**)	15 (**16%**)	
		ano	**ne**	
Jsou data o zaměstnancích sdílena s jinými firmami?	mikropodniky	11 (**23%**)	36 (**77%**)	
	malé podniky	41 (**27%**)	110 (**73%**)	
	střední podniky	18 (**20%**)	73 (**80%**)	
		ano	**ne**	
Jsou při ukončení pracovního poměru osobní údaje zaměstnance v přiměřené lhůtě vymazány, kromě ze zákona povinných informací?	mikropodniky	35 (**74%**)	12 (**26%**)	
	malé podniky	116 (**77%**)	35 (**23%**)	
	střední podniky	84 (**92%**)	7 (**8%**)	
BEZPEČNOST DOKUMENTACE				
		ano	**ne**	
Jsou tištěné dokumenty v uzamykatelné skříni nebo místnosti a ke klíčům mají přístup jen oprávněné osoby?	mikropodniky	38 (**81%**)	9 (**19%**)	
	malé podniky	116 (**77%**)	35 (**23%**)	
	střední podniky	76 (**84%**)	15 (**16%**)	
		ano	**ne**	
Jsou dokumenty po vypršení archivačních lhůt likvidovány?	mikropodniky	37 (**79%**)	10 (**21%**)	
	malé podniky	111 (**74%**)	40 (**26%**)	
	střední podniky	77 (**85%**)	14 (**15%**)	
		ano	**ano - bez postupů**	**ne**
	mikropodniky	12 (**26%**)	13 (**28%**)	22 (**45%**)

Existuje směrnice pro nakládání s osobními údaji, která obsahuje postupy pro řešení práv dotčených osob?	malé podniky	65 (**43%**)	49 (**32%**)	37 (**25%**)
	střední podniky	44 (**49%**)	25 (**27%**)	22 (**24%**)
		ano	**ne**	
Existují záznamy o provedených školeních zaměstnanců pro práci s osobními údaji?	mikropodniky	21 (**45%**)	26 (**55%**)	
	malé podniky	91 (**60%**)	60 (**40%**)	
	střední podniky	62 (**68%**)	29 (**32%**)	

Zdroj: vlastní zpracování

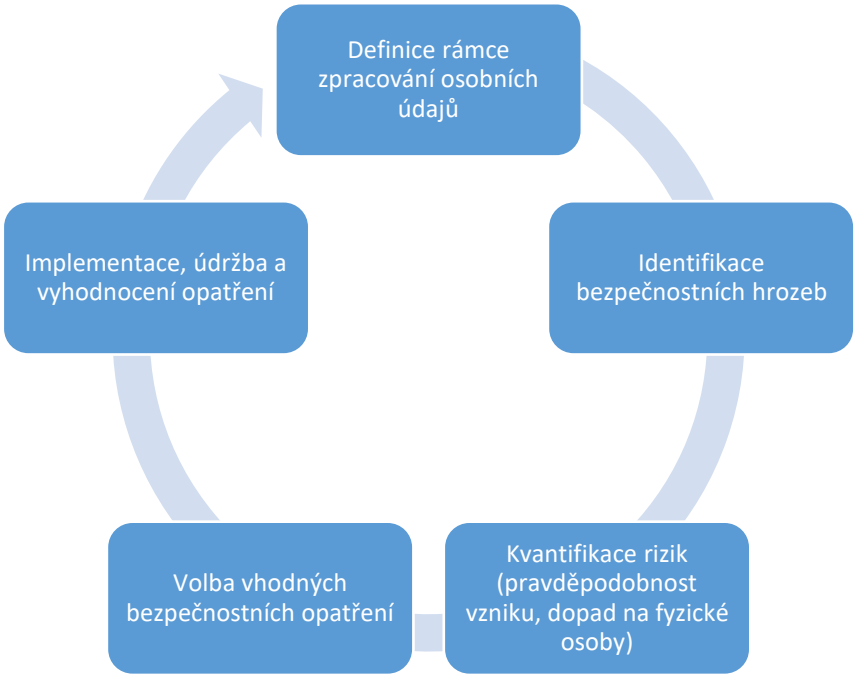
6 VÝSLEDKY

Management rizik je zásadním nástrojem mimo jiné také pro bezpečnost informací a jeho hlavním cílem je přijetí vhodných bezpečnostních opatření pro zvládání detekovaných rizik. Při uplatňování tohoto přístupu při zpracování osobních údajů je však třeba zvážit specifika tohoto zpracování, která vyžadují poněkud odlišný přístup jak při hodnocení rizik, tak i při jejich zpracování, akceptaci a komunikaci.

Ve standardním hodnocení rizik je závažnost rizika ohodnocena na základě jeho možných dopadů na organizaci. V případě zpracování osobních údajů jsou však dopady zvažovány s ohledem na práva a svobody fyzických osob. To je významný rozdíl, protože analýza dopadů musí být zaměřena na možné nežádoucí účinky, které mohou postihnout fyzické osoby (např. krádež identity, finanční ztráta, fyzická nebo psychická újma, ponižování, poškození dobrého jména, ohrožení života, atd.). Při provádění takové analýzy je třeba posoudit, zda je použité měřítko relevantní (např. počet zasažených osob). Dopad je totiž vysoký, i když způsobí vážné nežádoucí účinky pouze jedné fyzické osobě. Dalším problémem je, že pro kvantifikaci dopadu je třeba vzít v úvahu také možné sekundární účinky na práva a svobody fyzických osob.[21]

[21] Data Protection Working Party 29 Opinion 3/2014 on Personal Data Breach Notification.

Obrázek 6.1: Management rizik pro oblast ochrany osobních údajů



Zdroj: vlastní zpracování

Vzhledem k pojetí dopadů, které je specifické pro ochranu osobních údajů, se způsob řízení rizik také může lišit od standardního procesu hodnocení rizik. Pokud je výsledná pravděpodobnost určitého rizika nízká, nemusí být vždy správnou volbou rozhodnutí o akceptaci rizika, a to především v případě, že je možný výskyt závažných dopadů na určité fyzické osoby. V takovém případě by se správce nebo zpracovatel osobních údajů pravděpodobně měl vyhnout riziku, a to buď přehodnocením operací při zpracování, nebo využitím technologií zvyšujících ochranu osobních údajů (např. techniky anonymizace). I v jiných případech může být přijetí či nastavení konkrétních technických a organizačních opatření odlišné mezi standardním pojetím managementu rizik a managementem rizik při ochraně osobních údajů.

V oblasti managementu rizik při ochraně osobních údajů je především důležité definovat celkový rámec zpracování (např. kategorie osobních údajů, účel zpracování, oprávnění uživatelé atd.), který pak podpoří identifikaci možných hrozeb a rizik založených na dopadu na fyzické osoby. Příslušná technická a organizační opatření je vhodné přijmout s přihlédnutím ke specifikům oblasti ochrany osobních údajů.

Jak je znázorněno na obrázku 6.1, proces managementu bezpečnostních rizik při ochraně osobních údajů se v zásadě neliší od standardních modelů managementu rizik, musí být pouze zohledněna specifika zpracování osobních údajů, jak je uvedeno výše.

7 DISKUSE A ZÁVĚRY

Přístup založený na rizicích, tak jak je nastaven v GDPR, nepřipouští žádné výjimky týkající se velikosti organizace, dostupnosti zdrojů či jiných parametrů. Podobně jako velké organizace musí i MSP identifikovat úroveň rizika v závislosti na jeho povaze, rozsahu a kontextu zpracování osobních údajů. Definovat postup, který by vyhovoval všem organizacím, není zcela reálné. Konkrétní operace související se zpracováním osobních údajů se mezi správci údajů samozřejmě liší, stejně tak se bude lišit i celkový přístup jednotlivých správců k rizikům.

Ustanovení v GDPR přesahují pouhé přijetí konkrétních bezpečnostních opatření, podporují zavedení systému řízení bezpečnosti informací pro ochranu důvěrnosti, integrity, dostupnosti a odolnosti osobních údajů. MSP však někdy nevnímají korektně rizika související s ochranou osobních údajů, což vyplývá i z průzkumu, který byl pro účely tohoto dokumentu proveden a zpracován. Bylo by vhodnější, kdyby tyto organizace měly k dispozici metodiku, která by je přenesla přes propast mezi právními předpisy a správným vnímáním rizika a která by pomohla nastavit korektní procesy zpracování osobních údajů pro jednotlivé typy zpracovatelů.

Jednou z možností i pro MSP, jak prokázat shodu s GDPR, je certifikace (v České republice je certifikačním orgánem Český institut pro akreditaci, o.p.s.). GDPR ve čl. 42 stanovuje zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s GDPR. Je zde uvedeno, že specifické potřeby mikropodniků a malých a středních podniků budou zohledněny. Pro MSP to může být zajímavá cesta, protože se stále více spoléhají na technologie, výrobky a služby třetích stran a splnění požadavků GDPR může představovat garanci pro tyto partnery a zároveň konkurenční výhodu.

AFILACE

Příspěvek je zpracován jako jeden z výstupů výzkumného projektu „Implementace Obecného nařízení o ochraně osobních údajů v MSP“ v rámci oblasti IGA_AS_03_08, podporovaného interní grantovou agenturou AKADEMIE STING.

POUŽITÉ ZDROJE

[1] KRÁL, D. Management bezpečnosti informací v malých a středních podnicích. In: JEŽKOVÁ, R. a kol. Podnikání a management v malých a středních podnicích: teoretické aspekty a aplikace. 1. vyd. Brno: STING, spol. s r.o., 2015. 399 s. s. 224-269. ISBN 978-80-87482-30-8.

[2] NEZMAR, L. Praktický průvodce implementací, 1. vyd. Praha: GRADA Publishing, 2018, s.304, ISBN 978-80-271-0668-4.

[3] ŽŮREK, J. Praktický průvodce GDPR, 1. vyd. Praha: Anag, 2017, s. 224, ISBN 978-80-554-097-3.

[4] Aplikační výklad pro vymezení pojmů drobný, malý a střední podnikatel a postupů pro zařazování podnikatelů do jednotlivých kategorií. Czechinvest: Agentura pro podporu podnikání a investic [online]. 2014 [cit. 2018-10-24]. Dostupné z: http://www.czechinvest.org/data/files/definice-maleho-a-stredniho-podniku-2-1112.pdf

[5] Data Protection Working Party 29 Opinion 3/2014 on Personal Data Breach Notification, [online]. 2018 [cit. 2018-10-26]. Dostupné z http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[6] Definice malého a středního podnikatele. Czechinvest: Agentura pro podporu podnikání a investic [online]. c1994-2017 [cit. 2017-10-25]. Dostupné z: http://www.czechinvest.org/definice-msp.

[7] Guidelines for SMEs on the security of personal data processing. ENISA. European union agency for network and information security [online]. 2016 [cit. 2018-10-22]. Dostupné z: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing. ISBN 978-92-9204-209-7.

[8] Nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), In: eur-lex.europa.eu [online].© Evropská unie, http://eur-lex.europa.eu/, 1998-2018. [cit. 2018-10 18]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[9] Směrnice Evropského parlamentu a Rady 95/46 ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Úřední věstník EU, L 281, 23.11.1995. [online]. 1995 [cit. 2018-10-24]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31995L0046:CS:PDF.

[10] Úřad pro ochranu osobních údajů, Povinnost provádět posouzení vlivu na ochranu osobních údajů, [online]. © Praha 2013-2018, [cit. 23. 6. 2018].Dostupné z https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia.

[11] Zpráva o vývoji malého a středního podnikání a jeho podpoře v roce 2017. Ministerstvo průmyslu a obchodu [online]. 2018 [cit. 2018-10-24]. Dostupné z: https://www.komora.cz/legislation/78-18-zprava-o-vyvoji-maleho-a-stredniho-podnikani-a-jeho-podpore-v-roce-2017-t-30-7-2018/.

AUTOR

Ing. David Král, Ph.D., Katedra aplikovaných disciplín, AKADEMIE STING, o.p.s., Stromovka 1, 637 00 Brno, e-mail: kral@sting.cz.

AUTHOR

Ing. David Král, Ph.D., Department of Applied Disciplines, STING ACADEMY, Stromovka 1, 637 00 Brno, Czech Republic, e-mail: kral@sting.cz.