6 ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Úvodní poznámky

Správce a zpracovatel jsou na základě ustanovení § 13 odst. 1 zákona o ochraně osobních údajů *„povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i přímo k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů*".

Povinnost přijmout bezpečnostní opatření platí pro správce i zpracovatele i po ukončení zpracování osobních údajů. Použitelnost a praktický význam ustanovení o povinnosti přesahující dobu zpracování osobních údajů lze podle mého názoru nalézt výhradně při ukončení zpracování tím, že osobní údaje jsou předány jinému správci a samo toto předání je opatřením k zabezpečení osobních údajů (např. předání správci zajišťujícímu likvidaci, pokud ovšem není přejímající strana vůči předávajícímu správci zpracovatelem), nebo je známo, že alespoň část bezpečnostních opatření zůstane v platnosti i u nového správce či lze takovou okolnost důvodně předpokládat. Ochranná, bezpečnostní opatření musí být individualizovaná a přiměřená danému zpracování u toho kterého správce. Zákon tedy konkrétní způsoby ochrany a zabezpečení nestanoví, nicméně dává jisté vodítko, které oblasti rizik by měl správce osobních údajů posoudit a konkrétně vyhodnotit.[262] Rozsudek Nejvyššího správního soudu postuluje alespoň základní principy ochrany v tom směru; soud dovodil, že při ochraně osobních údajů je třeba automaticky aplikovat jisté, dnes již běžné standardy ochrany. V rozsudku soud uvádí, že dle jeho názoru existuje v oblasti bezpečnostních opatření k ochraně majetku obecně a při nakládání s osobními údaji, resp. jejich ochraně zvláště, určitý soubor bezpečnostních opatření považovaný za standard, aniž by musel být v zákoně výslovně vymezen.[263]

I když tedy existuje spíše snaha ujednotit tyto prostředky zabezpečení, můžeme se setkat s názory, které akcentují rozdílnost správců/zpracovatelů osobních údajů zejména subjektů soukromého práva. Srovnání možnosti způsobit těžký následek či porušení osobních údajů v rozdílně velké míře by mělo ospravedlnit nižší nároky na „drobné" správce/zpracovatele. Lze tak mít za to, že by veškeré podmínky a úroveň zabezpečení (tedy např. volba určitých technických

[262] BARTÍK, Václav, JANEČKOVÁ, Eva. Povinnosti osob při zabezpečení osobních údajů a možnost liberace, *Daně a právo v praxi*, 2013, č. 4, s. 46.

[263] Rozsudek Nejvyššího správního soudu ze dne 10. 5. 2006, čj. As 21/2005-105.

prostředků zabezpečení) měly být přiměřené konkrétním možnostem správce/zpracovatele osobních údajů.[264] Na druhou stranu v rámci veřejné správy si lze takovéto odlišnosti představit těžko, resp. úroveň zabezpečení a použitých prostředků ochrany osobních údajů by měla být standardem, kdy subjekt údajů by neměl mít pochybnosti o tom, že s jeho osobními údaji bude nakládáno nejen v souladu s ochranou poskytnutou právní úpravou. Dokonce si můžeme představit situaci, kdy subjekt údajů přímo očekává vysokou míru ochrany osobních údajů v držení veřejné správy, která je jistě vnímána jako solidní a důvěryhodný správce/zpracovatel.

Oč úspornější je legální vyjádření povinnosti, o to bohatší a košatější je její naplňování. Lze s nárokem na širší platnost konstatovat, že existuje jistý rámec pro řádné plnění povinnosti a že soubor opatření vyžadovaných pro takto zabezpečované zpracování osobních údajů je určován především prostředky a způsobem zpracování osobních údajů. Ty – až na výjimky u zákonem uložených zpracování – určuje z vlastního rozhodnutí sám správce. Jeho rozhodnutí, které vychází z jeho vlastních lidských, finančních, prostorových atd. možností, tak vytváří základní „operační prostor" pro bezpečnostní opatření. Obecným rámcem je to, že k řádnému s/plnění povinnosti musí být přijata odpovídající technická a organizační opatření.[265]

Význam slova „technická" je v tomto případě bezproblémový, slovo „organizační" je namístě chápat široce, ne pouze jako opatření zakotvená v organizační normě. Takový rámec je popsán v úvodním ustanovení čl. 46 směrnice 95/46, a to takto: „ochrana práv a svobod subjektů údajů v souvislosti se zpracováním osobních údajů vyžaduje, aby byla přijata příslušná technická a organizační opatření jak při přípravě zpracování, tak při jeho provádění, s cílem zajistit především bezpečnost a zabránit jakémukoli nepovolenému zpracování; tato opatření musí zajistit přiměřenou úroveň bezpečnosti odpovídající současnému stavu technického rozvoje a nákladům na jejich zavedení a použití (implementaci) vzhledem k rizikům při takovém zpracování a povaze údajů, které mají být chráněny."

6.1 Kategorie bezpečnostních opatření

Pokud bychom měli vystihnout podstatu bezpečnostních opatření, jež je správce (zpracovatel) jak na základě zákona, tak případně zvláštních právních předpisů povinen přijmout, pak je možné vymezit zhruba tři oblasti, v nichž je třeba

[264] MORÁVEK, Jakub. K zákazu sdružování osobních údajů, jejich zabezpečení a souvisejícím otázkám – část 2, *Zdravotnické fórum*, 2012, č. 11, s. 9.

[265] MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. vydání. Praha: ASPI, 2008, s. 262.

realizovat bezpečnostní opatření k zamezení změny, zničení či ztráty, neoprávněných přenosů nebo jiného neoprávněného zpracování, příp. jiného zneužití osobních údajů:

Oblast personální: jde zejména o omezení rozsahu osob, které mají do míst, kde dochází ke zpracování osobních údajů, a dále k informacím o zpracování a k údajům jako takovým přístup, spolu se zakotvením jejich povinnosti mlčenlivosti jak o zpracovávaných datech, tak o zpracování jako takovém a o jeho zabezpečení (i když ta plyne již ex lege), ale i o určení dalších pravidel k zajištění bezpečnosti zpracovávaných osobních údajů a informací o jejich zabezpečení, jako je například způsob nakládání s hesly pro přístup k údajům nebo povinnost uzamykat při odchodu kanceláří, ukládat spisy na určená místa a odhlašovat se z PC. Jde-li o povinnost mlčenlivosti, tato vyplývá z § 15 zákona o ochraně osobních údajů. Dále lze subsumovat pod tuto kategorii vymezení případů, kdy mohou dané osoby přístup realizovat spolu s jasnou specifikací účelů, pro jejichž naplnění mohou s osobními údaji disponovat, a rámcového označení těchto dispozic.[266]

Do oblasti personální bezpečnosti ochrany osobních údajů lze zahrnout povinnosti správce a zpracovatele posoudit rizika na základě ustanovení § 13 odst. 3 písm. a) a b) zákona o ochraně osobních údajů.

Dle prvního z těchto ustanovení je nutno posoudit „rizika týkající se splnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům", čemuž odpovídá současně v případě automatizovaného zpracování povinnost správce dle § 13 odst. 4 písm. b) a c) zákona, tj. zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby, a pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. Ze znění § 13 odst. 4 zákona přitom vyplývá, že se nejedná o taxativní výčet opatření pro zajištění bezpečnosti zpracování.[267]

Z ustanovení § 13 odst. 3 písm. b) potom vyplývá povinnost správce a zpracovatele posoudit rizika „zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování".

Oblast technická: čl. 17 směrnice 95/46 ukládá povinnost, aby členské státy stanovily, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, ná-

[266] MORÁVEK, Jakub. K zákazu sdružování osobních údajů, jejich zabezpečení a souvisejícím otázkám – část 2, *Zdravotnické fórum*, 2012, č. 11, s. 7.

[267] Z rozhodovací činnosti ÚOOÚ: K zabezpečení osobních údajů (čj. VER-3280/08-34), *Věstník Úřadu pro ochranu osobních údajů*, 2009, č. 53, s. 3063.

hodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování. Tato opatření mají zajistit, s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny.

Zákon v ustanovení § 13 odst. 2 ukládá, že „*správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy*". Opatření musí být v souladu se zákonem o ochraně osobních údajů, ale také s jinými právními předpisy. Vzhledem k tomu, že zákonodárce použil velmi obecnou formulaci, lze jistě přijmout myšlenku, že nezamýšlel přesně stanovit formu a obsah požadovaného dokumentu nebo dokumentů. I když by asi vhodnější bylo, aby pravidla ochrany osobních údajů byla shromážděna do dokumentu jednoho, lze si jistě představit i situaci jinou, tedy že příslušný komplex pravidel bude obsahem několika rozdílných interních předpisů správce (zpracovatele), které ve svém komplexu právě taková pravidla tvoří. Zdá se, že v praxi bude četnější právě druhá z naznačených možností, kdy např. jeden dokument obsahuje pravidla obecné (počítačové) bezpečnosti a v dalších dokumentech jsou uvedena další pravidla pro nakládání s osobními údaji.[268]

Oblast výpočetní techniky: zejména u případů automatizovaného zpracování osobních údajů prostřednictvím počítače jde o pořízení odpovídajícího softwaru, který zamezí přístupu jiným než správcem určeným osobám, dále do této kategorie spadá logování (to nicméně prolíná všemi naznačenými kategoriemi). Bezpečnost bude většinou zajištěna specifickými prostředky výpočetní techniky, tedy přístupovými právy, a to individuálními s případným rozlišením specifických oprávnění, jako jsou např. oprávnění pouze nahlížet, měnit konkrétní záznam apod.

Na oblast technickou i oblast výpočetní techniky lze pak vztáhnou povinnost správce a zpracovatele kladenou jim § 13 odst. 3 písm. c) zákona, podle kterého tito posuzují rizika týkající se „zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje".

[268] BARTÍK, Václav, JANEČKOVÁ, Eva. Bezpečnost osobních údajů podle zákona o ochraně osobních údajů, *Právní rozhledy*, 2010, č. 23, s. 840.

6.2 Zabezpečení automatizovaného zpracování osobních údajů

V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel na základě ustanovení § 13 odst. 4 zákona o ochraně osobních údajů v rámci opatření povinen zajistit některé další povinnosti. Toto ustanovení je třeba posuzovat kontextuálně, a nikoliv vytrženě ze smyslu a účelu povinností stanovených v § 13 odst. 1 zákona. Povinnosti uvedené pod § 13 odst. 4 písm. a) a b) zákona pouze zpřesňují obecnou povinnost správce přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům v případě, že se jedná o automatizovaný způsob zpracování. Je tedy nutné volit nejen obecná organizační opatření, ale také metody, které taková opatření promítnou do automatizovaných zpracování prostředky, které mu adekvátně odpovídají. Účelem a smyslem ustanovení je zajistit, aby správce mohl zjistit, jakým způsobem bylo s údaji při automatizovaném zpracování nakládáno, a to takovým způsobem, že o přístupech budou existovat elektronické záznamy, tzv. „logy".

Současně to však neznamená, že by nezbytně musely existovat záznamy o přístupech v rámci jednoho informačního např. databázového systému ke konkrétní datové větě, i když ani taková možnost není vyloučena a bude vždy záviset na každém individuálním vyhodnocení rizik ve vztahu k závažnosti chráněných dat, které je správce povinen posoudit podle odstavce 3, když povinnost podle písm. c) je možné plnit i v kombinaci s vhodnými organizačními opatřeními. Povinnost stanovená v odstavci 4 je upřesňující v tom smyslu, že chránit je třeba nejen samotná „aktivní" automatizovaná zpracování probíhající na prostředcích výpočetní techniky, ale také individuální datové nosiče, na nichž jsou např. uchovávány zálohové soubory, a že tato ochrana musí být systémová a odpovídající vyhodnoceným rizikům.[269]

6.3 Zaměstnanci správce či zpracovatele

Jak již bylo letmo zmíněno výše, na základě ustanovení § 14 zákona o ochraně osobních údajů „zaměstnanci správce nebo zpracovatele a jiné osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném". Toto ustanovení tedy určuje povinnosti i dal-

[269] JANEČKOVÁ, Eva. Pracovní právo – osobní údaje, *Daně a právo v praxi*, 2014, č. 2, s. 10.

ším osobám, rozdílným od správců nebo zpracovatelů. Jedná se o jejich zaměstnance nebo o jiné osoby, které pro ně vykonávají zpracování osobních údajů. Ustanovení tak vzhledem k použitému termínu „osoby" stíhá jak osoby fyzické, tak právnické. U osob fyzických se bude především jednat o zaměstnance v pracovním poměru ke správci nebo zpracovateli na základě zvláštního právního předpisu.[270]

Vzhledem ke stanovené povinnosti je zřejmé, že správce nebo zpracovatel musí dotčeným osobám určit podmínky zpracování. Ostatně tak vyplývá i z důvodové zprávy k návrhu zákona o ochraně osobních údajů, kde je uvedeno: „*tímto ustanovením je vyloučeno, aby osoby, kterým nedá správce nebo zpracovatel souhlas, jakkoli zpracovávaly osobní údaje. Správce, resp. zpracovatel musí stanovit též rozsah oprávnění, v němž určitá osoba má k osobním údajům přístup a může je zpracovávat.*"[271]

Pokud se týká zaměstnanců, je zřejmé, že zaměstnanec musí takové pokyny obdržet. Asi nejběžnější formou takových pokynů bude jejich zařazení do pracovní náplně zaměstnance nebo jejich obecné vyjádření v některém z interních aktů řízení správce nebo zpracovatele. Interním aktům řízení by měly zůstat vyhrazeny otázky spíše obecné, platné pro všechny typy zpracování, a jejich individualizace by měla být právě otázkou pracovní náplně či pokynů k práci s konkrétním zpracovávaným souborem osobních údajů na základě např. počítačového programu.[272]

Ustanovení § 14 zákona je tak bezprostředně spjato jak se zaměstnanci, kteří se do styku s osobními údaji dostávají jako s nedílnou součástí svého pracovního zařazení při plnění pracovních úkolů (např. pracovníci řešící správní řízení, mzdová účetní, pracovníci personálních oddělení atd.), tak i případně se zaměstnanci, kteří spíše zajišťují technické zázemí ochraně osobních údajů (pracovníci informačních technologií, správci počítačových sítí atd.). Toto ustanovení zákona tak můžeme chápat i jako vyjádření jedné ze základních povinností zaměstnance vyplývající z pracovního poměru.[273]

„Podmínkami" ve smyslu ustanovení § 14 zákona o ochraně osobních údajů se tak rozumí zřejmě jednotlivé organizační pokyny zaměstnavatele spočívající zejména ve stanovení vedoucích pracovníků a určení odpovědnosti konkrétních osob za jednotlivé kroky v rámci zpracování osobních údajů. Řadíme sem i pokyny týkající se využití konkrétních prostředků pro zpracování osobních údajů

[270] § 33 a násl. zákoníku práce.

[271] Důvodová zpráva k zákonu č. 101/2000 Sb., zvláštní část.

[272] BARTÍK, Václav, JANEČKOVÁ, Eva. Bezpečnost osobních údajů podle zákona o ochraně osobních údajů, *Právní rozhledy*, 2010, č. 23, s. 842.

[273] Srov. např. § 38 odst. 2 písm. b) zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

a vhodného způsobu práce s nimi, tedy již konkrétní pokyny ohledně např. používání přístupových hesel, zamykání kanceláří apod. Zajištění znalosti zásad zacházení s osobními údaji je pak ošetřeno zejména vnitřními předpisy, které stanoví povinnost řádně nakládat s osobními údaji jako součást pracovní kázně příslušných zaměstnanců.[274]

Výše uvedené je v souladu s judikaturou Nejvyššího soudu,[275] podle níž obhajobu spočívající v tom, že nosiče osobních údajů byly odneseny omylem, resp. že třetí osoba využila okamžiku snížené pozornosti, Nejvyšší soud jednoznačně odmítl s odkazem na povinnosti stanovené v interním předpise, konkrétně povinnost přijmout opatření potřebná k tomu, aby se s údaji získanými z informačního systému nemohla seznámit osoba, která nemá potřebné oprávnění. Zakotvení obdobné povinnosti v interním dokumentu je, jak již bylo výše uvedeno, typickým příkladem plnění povinnosti správce osobních údajů podle § 13 zákona, čímž současně vznikají dotčeným zaměstnancům povinnosti ve smyslu § 14 zákona o ochraně osobních údajů.[276]

6.4 Povinnost mlčenlivosti

Zákon o ochraně osobních údajů zavádí v ustanovení § 15 tzv. obecnou povinnost mlčenlivosti. Povinnost mlčenlivosti, která se dříve uplatňovala v rámci zachování tzv. tajemství (lékařské tajemství, advokátní tajemství, bankovní tajemství) jen v určitých oborech, je nyní stanovená jako obecná povinnost pro všechny, kteří s osobními údaji pracují. Zásada mlčenlivosti se tím vztahuje na každého, kdo přijde s osobními údaji do styku, a souvisí s ochranou osobnosti subjektu údajů (ochrana před zasahováním do soukromí).[277]

Povinnost mlčenlivosti nijak nezbavuje správce odpovědnosti za zabezpečení osobních údajů, stejně tak jako obecné stanovení místa výkonu práce. Jak již bylo uvedeno, účelem povinnosti dle § 13 odst. 1 zákona není primárně to, aby správce osobních údajů přijal formálně bezpečnostní předpisy, ale zajištění toho, aby nedošlo k neoprávněnému přístupu k osobním údajům, a tím naplnění práva subjektu údajů na ochranu jeho soukromí.[278]

---

[274] KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck, 2012, s. 245.

[275] Rozsudek Nejvyššího soudu ze dne 26. 1. 2010, čj. 4 Tdo 1209/2009.

[276] Shodně stanoví článek 7 Úmluvy 108, mj. že je třeba učinit vhodná bezpečnostní opatření proti náhodnému zničení, jakož i neoprávněnému přístupu, změnám nebo šíření.

[277] BĚLECKÝ, Miroslav. Ochrana osobních údajů a BOZP, 2. část, *Bezpečnost a hygiena práce*, 2012, č. 2, s. 11.

[278] BARTÍK, Václav, JANEČKOVÁ, Eva. Povinnosti osob při zabezpečení osobních údajů a možnost liberace, *Daně a právo v praxi*, 2013, č. 4, s. 48.

Konkrétně zákon v ustanovení § 15 odst. 1 stanoví, že „*zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací*".

Obecnou povinností mlčenlivosti dle zákona o ochraně osobních údajů ovšem nejsou dotčené osoby zbaveny povinnosti mlčenlivosti, kterou jim stanoví zvláštní zákony.[279] Toto v praxi znamená, že povinnost mlčenlivosti zakotvená v zákoně o ochraně osobních údajů nenahrazuje povinnost mlčenlivosti, kterou stanoví jiné zákony, a že povinnost mlčenlivosti stanovená těmito jinými zákony platí vedle povinnosti mlčenlivosti podle zákona o ochraně osobních údajů. Pokud má tedy nějaká fyzická osoba povinnost mlčenlivosti nejen podle zákona o ochraně osobních údajů, ale i podle jiných zákonů, je povinna i tyto povinnosti mlčenlivosti podle jiných zákonů zachovávat. Obě totiž stojí vedle sebe a jedna nenahrazuje ani nevylučuje druhou.[280]

Do popředí v souvislosti s povinností zachovávat mlčenlivost[281] vystupuje ve veřejnoprávní rovině problematika zachování mlčenlivosti o informacích, které se fyzické osoby dozvědí v souvislosti se svou veřejnou funkcí (např. zastupitelé obcí a krajů, poslanci, senátoři). Podle § 15 zákona o ochraně osobních údajů platí, že i *osoby, které přicházejí do styku s osobními údaji u zpracovatele či správce,* jsou povinny zachovávat mlčenlivost. Tak zastupitelé obce, kteří mají dle zákona o obcích právo nahlížet do zápisů z jednání zastupitelstev, nemohou získané informace, potažmo osobní údaje, dále šířit např. elektronickou formou.[282]

Povinnost zachovávat mlčenlivost se ovšem nevztahuje na informační povinnost podle zvláštních zákonů.[283] Nebrání také v plnění informační povinnosti správců údajů.

[279] Například zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů, či zákon č. 89/1995 Sb., o státní statistické službě, ve znění pozdějších předpisů.

[280] BARTÍK, Václav, JANEČKOVÁ, Eva. Mlčenlivost a některé aspekty při nakládání s informacemi, *Řízení školy*, 2013, č. 12, s. 4.

[281] Povinnost mlčenlivosti není v zákoně o ochraně osobních údajů definována.

[282] Srov. rozhodnutí Úřadu pro ochranu osobních údajů 2/06/PŘ.

[283] Například ustanovení § 11 zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů nebo již probíraného vztahu § 8a zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

6.5 Závěr

Z výše naznačených východisek je patrné, že s ochranou osobních údajů úzce souvisí také problematika jejího technického zabezpečení.

Ačkoli se může zdát vše jasné v ohledu seznámení zaměstnanců s pravidly pro zabezpečení ochrany osobních údajů, nelze podcenit ani lidský faktor, který hraje důležitou úlohu. I sebelepší zabezpečení v rovině technické nemusí být dostatečné, pakliže selžou účinné nástroje personální politiky. Jinými slovy, zaměstnanci, jejichž pracovní náplň bude úzce souviset s osobními údaji, by měli být vždy řádně proškolování, seznámeni s vnitřními předpisy aktivním způsobem tak, aby dokázali zásady ochrany osobních údajů aplikovat v reálných situacích.

Excesům spočívajícím v trestné činnosti zaměstnance nebo v zásahu vyšší moci sice nelze stoprocentně zabránit, nicméně i tato rizika lze vhodně zvolenými prostředky ochrany a adekvátním systémem kontrolní činnosti nadřízených zaměstnanců značně eliminovat.