Mendelova univerzita v Brně
Provozně ekonomická fakulta

Ochrana informací v praxi obchodní společnosti

Diplomová práce

Vedoucí práce:

JUDr. Hana Kelblová, Ph.D. **Bc. Kateřina Žáčková**

Brno 2017

Chtěla bych poděkovat paní JUDr. Haně Kelblové, Ph.D. za vstřícnost, odborné vedení a cenné rady při psaní této diplomové práce.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Ochrana informací v praxi obchodní společnosti** vypracovala samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Jsem si vědoma, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 19. května 2017 _____

Abstract

Žáčková, K., Protection of information in the practice of a business company. Thesis. Brno: Mendel University in Brno, 2017.
This diploma thesis deals with the protection of information of the entrepreneur in a particular IT company. Attention was paid first to the area of protection of business secrets, know-how and confidential information towards employees of the company and to its clients and business partners, as well as to the protection of employee's and customer's personal data. Based on an analysis of internal processes and documents, contracts with employees, customers and business partners, shortcomings were identified and recommendations were subsequently proposed in line with valid legislation in the Czech Republic. In conclusion, the economic impacts were assessed not only from the identified shortcomings but also from the introduction of the proposed recommendations.

Keywords

Protection of information, trade secret, confidential information, know-how, personal data, commercial communication.

Abstrakt

Žáčková, K., Ochrana informací v praxi obchodní společnosti. Diplomová práce. Brno: Mendelova univerzita v Brně, 2017.
Tato diplomová práce se zabývá ochranou informací podnikatele v konkrétní obchodní společnosti zabývající se IT. Pozornost byla věnována nejdříve oblasti ochrany obchodního tajemství, know-how a důvěrných informací vůči zaměstnancům společnosti i vůči jejím klientům a obchodním partnerům, dále oblasti ochrany osobních údajů zaměstnanců a zákazníků. Na základě analýzy interních procesů a dokumentů, smluv se zaměstnanci, zákazníky a obchodními partnery byly zjišťovány nedostatky a následně navržena doporučení v souladu s platnou legislativou České republiky. V závěru byly zhodnoceny ekonomické dopady nejen ze zjištěných nedostatků, ale také ze zavedení navržených doporučení.

Klíčová slova

Ochrana informací, obchodní tajemství, důvěrné informace, know-how, osobní údaje, obchodní sdělení.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

S informacemi pracuje každý podnikatel bez ohledu na velikost jeho firmy či obor podnikání. Mnohé z těchto informací pro něj představují velmi hodnotný majetek, díky němuž je schopen vyrábět nebo poskytovat služby lépe, levněji nebo rychleji než konkurence. Je zřejmé, že tyto informace je třeba chránit.

Mnoho informací podnikatel chránit musí, ať už mu tato povinnost vyplývá ze smlouvy nebo ze zákona.

V běžné podnikatelské praxi je však tato problematika velmi podceňovaná a ochraně informací se zdaleka nevěnuje taková pozornost, jakou by si zasloužila. Podnikatelé se tak často vystavují mnoha rizikům ve formě ztráty dobrého jména či konkurenční výhody, ale také vysokým pokutám nebo sankcím ze strany kontrolních orgánů.

Tato práce se zabývá ochranou informací v konkrétní společnosti zabývající se IT. Je to oblast, kde informace mají obrovský význam a jejich ochrana je zde proto klíčová.

V práci bude zkoumáno, do jaké míry si je společnost těchto skutečností vědoma, jak ochraňuje svá cenná interní data, ale také informace klientů a obchodních partnerů. Pozornost bude věnována také otázce, zda případná pochybení plynou z neznalosti legislativy, nedůslednosti nebo z jiných důvodů a zda jsou ve společnosti jasně nastavená pravidla, se kterými jsou všichni zaměstnanci seznámeni.

Ochrana informací je stále častěji diskutované téma a je všeobecně známo, že informace je potřeba chránit, ale jak vypadá realita v každodenní podnikatelské praxi?

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je definovat nedostatky v oblasti ochrany informací podnikatele v konkrétní obchodní společnosti zabývající se IT a na základě jejich analýzy navrhnout vhodná řešení respektující současnou právní úpravu České republiky. Splnění hlavního cíle bude dosaženo prostřednictvím několika postupných kroků.

Prvním z nich bude na základě analýzy interních norem a smluv uzavíraných se zaměstnanci, dodavateli a odběrateli v obchodně právním vztahu, případně jinými subjekty, vyhodnotit, jak je ochrana informací zabezpečena vůči těmto osobám a v případě zjištění nedostatků navrhnout úpravy.

Druhým krokem bude návrh interního pracovněprávního dokumentu – pracovního řádu, upřesňujícího způsob ochrany informací ve firmě.

Třetím krokem bude zhodnocení zajištění ochrany informací, know-how a obchodního tajemství ve vztahu k externím odběratelům.

Čtvrtý krok bude spočívat ve zhodnocení ekonomických dopadů plynoucích nejen z možných nedostatků, ale také ze zavedení navržených doporučení.

2.2 Metodika

Zdrojem informací pro tuto diplomovou práci bude česká a zahraniční odborná literatura, zákony, tuzemské i zahraniční studie a jiné internetové zdroje zabývající se danou problematikou.

Nejdříve bude provedena analýza současné situace ve vybrané společnosti, tzn. zjištění, jakým způsobem jsou informace chráněny, rozbor smluv a analýza nedostatků. Poté budou formulována konkrétní doporučení a návrhy smluvních ujednání v souladu s českou legislativou.

Součástí bude návrh pracovního řádu pro konkrétní společnost upravující podmínky a způsoby ochrany informací.

Pozornost bude věnována také ekonomickým dopadům v případě nedodržení povinností vyplývajících z právních ujednání či vad těchto ujednání a také ekonomické náročnosti aplikace doporučení uvedených v této diplomové práci.

Výsledky budou formulovány jako doporučení pro konkrétní firmu, budou je však moci využít i jiní podnikatelé zabývající se podobnou problematikou.

Při zpracování tématu bude pro dosažení odpovídajících výsledků využito gramatického, teleologického, slovního a logického výkladu a rovněž metody analýzy a syntézy. Při srovnání současné právní úpravy a podnikové praxe je nutná aplikace metody komparace.

3 Literární rešerše

Informace mají v lidské společnosti obrovskou hodnotu již od nepaměti. Jejich význam a význam jejich ochrany neustále roste především s neustále probíhajícím pokrokem v oblasti informačních technologií. (Maisner, 2011, s. 108)

Dle mnoha autorů bude 21. století stoletím informační společnosti. Informace nás obklopují při každodenních činnostech, každý z nás pracuje s nejrůznějšími druhy informací. Proces získávání a zpracování informací je drahá a časově náročná činnost. Informace ale firmám často přinášejí větší zisky než pouhá výrobní činnost, a proto již většina organizací pochopila, že informace jsou firemním zdrojem stejně tak významným jako materiál, půda, pracovníci aj. Nároky na ochranu dat proto rostou obrovským tempem. (Šilerová a kolektiv, 2016, s. 13) (Webster, 2006)

Pojmy informace, data či údaje bývají v obecném povědomí často považovány za synonyma. Z pohledu informačních technologií ale mezi nimi existuje zásadní rozdíl. Definic existuje celá řada, mezinárodní definice pojmu informace zní: „Informace je význam, který člověk přisuzuje datům. Data jsou obrazem vlastnosti subjektu, vhodně formalizované pro přenos, interpretaci nebo zpracování prostřednictvím lidí nebo automatů“. Informaci lze také jednodušeji definovat jako sdělení pojednávající o určité skutečnosti. (Šilerová a kolektiv, 2016, s. 14) Data jsou v podstatě stavebním kamenem informací a informace bývají přenášeny v podobě dat. (Maisner, 2011, s. 109)

Z právního hlediska však dle mnoha autorů nemá smysl pojmy rozlišovat, a proto i v následujícím textu s nimi bude nakládáno jako se synonymy. (Maštalka, 2008, s. 5)

3.1 Informace ve firmě a jejich ochrana

Ve firmě se lze setkat se značným množstvím různých informací. Jde o informace různého charakteru, podoby či důležitosti. Obecně se informace v obchodní společnosti týkají:

- společnosti samotné a procesů v ní (informace o finančním stavu firmy, výrobní postupy, vnitřní předpisy, výsledky výzkumu apod.)
- zaměstnanců (jméno, datum narození, informace pro výplatu mezd či platbu pojistného apod.)
- třetích stran, především obchodních partnerů a zákazníků (kontaktní údaje a nejrůznější informace získané během jednání)

Některé informace jsou pro podnikatele natolik významné, že si zaslouží zvláštní pozornost. Jedná se především o informace o výrobních postupech, tajných recepturách nebo o nejrůznější speciální znalosti a poznatky, které ostatní subjekty na trhu neznají, na jejichž základě je podnikatel schopen vyrábět nebo poskytovat

služby efektivněji. Takové informace pro firmu představují významnou konkurenční výhodu a je v jejím zájmu tyto informace chránit. (Čada, 2010, s. 3)

Jiné informace podnikatel naopak chránit musí, přičemž tato povinnost může vyplývat ze zákona nebo ze smlouvy. Zde jde zejména o informace o zaměstnancích nebo o informace, které se dozvěděl v rámci spolupráce s jiným subjektem.

Ochrana informací a podnikových dat hraje významnou roli ve všech společnostech bez ohledu na jejich velikost, přičemž největším rizikům jsou vystaveny malé a střední firmy, které tuto skutečnost nejčastěji podceňují. (Saeed, 2011) Mezi tato rizika nepatří pouze ztráta či zneužití daných informací, ale také ztráta dobrého jména, konkurenční výhody či nejrůznější sankce. (Hinder, Brennan, 2014)

Prostředky pro ochranu firemních informací obecně jsou rozmanité a jejich použití je závislé na charakteru daných informací, ale též na aktuální situaci na trhu, rozvoji vědy, právním systému či morálních zásadách. (Maisner, 2011, s. 127)

Pro efektivní ochranu firemních informací je podle Maisnera nutná kombinace ochrany fyzické a právní. Jedna bez druhé nezajišťují dostatečnou ochranu, kterou si tyto informace vyžadují. (2011, s. 128)

3.2 Fyzická ochrana informací ve firmě

Stále častější využívání informačních technologií pro správu informací s sebou přináší i mnoho rizik v podobě jejich ztráty, zneužití nebo nedostupnosti. Jako v mnoha jiných oblastech, tak i v oblasti ochrany informací představují nejrizikovější faktor lidé. (Rodryčová, Staša, 2000, s. 14) Společně se zvyšujícím se počtem pracovníků pracujících s informacemi rostou i příležitosti pro destrukci, odcizení či využití informací pro vlastní prospěch. (Čada, 2010, s. 189)

Ochrana firemních informací si vyžaduje aktivní přístup ze strany zaměstnavatele. Ten by měl zajistit omezený přístup k chráněným informacím. Citlivá data by měla být uložena na heslovaných nosičích, posílána v šifrované podobě nebo uložena tak, aby k nim měli přístup pouze určení zaměstnanci. (Jansa, Otevřel, 2014, s. 77) Zde lze zařadit zejména uchovávání informací na chráněných místech (např. v závodu s ostrahou, v sejfu, za uzamykatelnými dveřmi), využívání zabezpečené počítačové sítě či speciálního software pro ochranu a šifrovaný přenos informací. (Černá a kolektiv, 2016, s. 207)

Podstatným opatřením je také určení vlastníků či osob zodpovědných za jednotlivé dokumenty a informace. (Saeed, 2011)

3.3 Právní ochrana informací ve firmě

Právní ochrana firemních dat je roztříštěna do celé řady právních předpisů. Nalezneme ji především v novém občanském zákoníku (dále jen „NOZ“), trestním zákoníku (dále jen „TZ“), v zákoníku práce (dále jen „ZP“) a v zákoně o ochraně osobních údajů (dále jen „ZoOOÚ“). (Maisner, 2011, s. 113)

3.3.1 Ochrana informací daná zákonem

Některé informace jsou, po splnění pevně daných pojmových znaků, chráněny přímo ze zákona. Ve firemním prostředí se jedná především o institut obchodního tajemství, důvěrných informací a osobních údajů. Blíže o těchto skupinách údajů v dalším textu.

Zákonem je upravena také pracovněprávní ochrana informací ve firmě. Mezi základní povinnosti zaměstnance definované v § 301 ZP patří *„povinnost řádně hospodařit s prostředky svěřenými jim zaměstnavatelem a střežit a ochraňovat majetek zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a nejednat v rozporu s oprávněnými zájmy zaměstnavatele“*. Z toho lze mylně vyvozovat i povinnost chránit podnikatelova data. O výslovnou povinnost mlčenlivosti se však nejedná. Tu mají uloženou pouze zaměstnanci v profesích taxativně uvedených v § 303 ZP, jedná se např. o zaměstnance Policie České republiky, České národní banky či soudů. (Maisner, 2011, s. 138)

Ochrana informací ve vztahu k zaměstnancům je podnikateli umožněna díky možnosti smluvní úpravy povinností zaměstnanců. Tyto vztahy se poté řídí NOZ. Zaměstnavatel je přesto do značné míry stále limitován ZP. Nesmí např. zaměstnancům ukládat peněžní postihy za porušení jejich povinností (s výjimkou náhrady škody) ani s nimi sjednávat jakékoliv formy zajištění (s výjimkou smluvní pokuty v rámci konkurenční doložky). (Galvas, 2015, s. 383) (Maisner, 2011, s. 138) Porušení povinnosti mlčenlivosti však může být považováno za podstatné porušení pracovních povinností zaměstnance a může tak být důvodem k okamžitému zrušení pracovního poměru. (Jansa, Otevřel, 2014, s. 80)

3.3.2 Smluvní ochrana informací

Mnohdy je vhodné zajistit ochranu informací smluvně. Důvodem smluvní ochrany bývá především obecná podoba právní úpravy, která často není schopna reflektovat konkrétní potřeby daného případu. Při případném soudním řízení je navíc často obtížné prokázat, zda šlo či nešlo o dané chráněné informace, protože zákon nabízí pouze obecnou, široce pojatou definici. Smluvní úprava umožňuje přesnější definici daných pojmů a stanovení podmínek vyhovujících konkrétnímu případu. (Maisner, 2011, s. 140)

Situace, kdy je podle Maisnera smluvní úprava ochrany dat velmi vhodná, jsou zejména tyto:

- Vyžaduje to povaha smluvního vztahu – např. v případě smlouvy o dílo na komplikovanou dodávku, na které bude pracovat mnoho pracovníků či subdodavatelů.
- Strany uzavírají více smluv – je praktické uzavřít jednu smlouvu, která upravuje ochranu informací pro všechny smlouvy vzniklé mezi určitými smluvními stranami.
- Obtížně vyčíslitelná náhrada škody nebo výše nemajetkové újmy – v takových případech je vhodné sjednat smluvní pokutu, která náhradu škody nahrazuje nebo doplňuje.

- Vyjednávání o uzavření smlouvy – předsmluvní ochrana informací je sice zakotvena přímo v zákoně, v případě jednání o uzavření smlouvy, při kterém dochází k výměně citlivých informací, je však vhodné ochranu informací a její podmínky zajistit i smluvně.
- Smluvní strana je povinna chránit data třetích osob – typickým příkladem může být správa informačních systémů bank.
- Informace jsou přímo předmětem smluvního vztahu – jedná se o smlouvu mezi správcem a zpracovatelem, předmětem smlouvy je jakékoliv nakládání s daty, např. analýza, ochrana apod. (2011, s. 142)

Podoba smlouvy pro ochranu informací není zákonem definována. Může se jednat jak o dodatek ke smlouvě nebo jen část smluvního ujednání, tak o samostatnou smlouvu, často nazývanou NDA (non-disclosure agreement). Většina autorů (Maisner, 2011, s. 144) (Jansa, Otevřel, 2014, s. 163) doporučují ve smluvním ujednání vždy zvážit následující:

- Přesné vymezení chráněných informací – nevhodná jsou ujednání, která chrání veškeré informace, které se subjekt při plnění smlouvy dozví, zejména je-li to dále spojeno s vysokou smluvní pokutou. Je totiž zřejmé, že se strany při plnění smlouvy o sobě navzájem dozví velké množství informací, mnoho z nich však bude všeobecně známo nebo nebudou pro podnikatele natolik významné. Musí se jednat o informace, u kterých je rozumné, aby byly ochraňovány.
- Označení chráněných informací – doporučuje se stanovit, zda a jak budou chráněné informace označeny. Vhodné je např. složku s takovými dokumenty nebo datový nosič označit štítkem „obchodní tajemství“ či „důvěrné informace“ apod. Zároveň ale není vhodné z takového označení činit nutnou podmínku ochrany, protože je v praxi velmi těžké zajistit, aby u všech údajů toto označení vždy bylo. U informací, které jsou pro firmu opravdu důležité, je to však žádoucí.
- Rozsah a způsob ochrany – je dobré upřesnit okruh osob, které budou s informacemi pracovat a také způsob technické ochrany. Je vhodné ve smlouvě myslet i na případy, kdy s informacemi budou muset pracovat i jiné osoby, např. auditoři, právní zástupci apod.
- Časový rozsah ochrany – informace by měly být chráněny jen po dobu, po kterou má jejich ochrana pro smluvní strany význam. Je tedy nevhodné ujednat ochranu platnou na neomezenou dobu. Některé informace se postupem času můžou stát všeobecně známými, jiné pozbydou významu po splnění smlouvy.
- Výslovný závazek stran údaje chránit – i když se může zdát, že se jedná o samozřejmost, je tato podmínka pro ochranu dat klíčová. Bez tohoto prohlášení totiž neexistuje povinnost informace chránit, a tedy není možné se poté dovolávat jejich ochrany. Výjimkou jsou obchodní tajemství, důvěrné informace a osobní údaje, které, pokud jsou splněny všechny pojmové znaky, jsou chráněny ze zákona.

- Stanovení náhrady škody – náhrada škody poškozenému náleží ze zákona. Nevýhodou ale je, že poškozený má povinnost dokázat vznik a výši škody, což bývá velmi obtížné, v mnoha případech dokonce až nemožné. Proto je vhodnější sjednat místo náhrady škody smluvní pokutu (viz dále).

  V případě smlouvy se zaměstnancem je zaměstnavatel limitován ZP. Rozsah náhrady škody je dán formou zavinění, druhem odpovědnosti a funkcí zaměstnance. V zásadě je zaměstnanec povinen nahradit celou skutečnou škodu, maximálně však do výše 4,5násobku průměrného měsíčního výdělku zaměstnance. Ušlý zisk zaměstnanec povinen nahradit není. Tyto limitace neplatí v případech, kdy je škoda způsobena úmyslně, v opilosti nebo v důsledku požití jiných omamných látek. Zvláštní povinnosti mají vedoucí zaměstnanci. (Galvas, 2015, s. 690)
- Ujednání o smluvní pokutě – ujednání o smluvní pokutě je poměrně výhodným fakultativním ujednáním. V případě porušení povinnosti náleží poškozené straně smluvní pokuta bez ohledu na to, zda mu porušením této povinnosti druhou smluvní stranou vznikla škoda či nikoliv.

  Podle § 2050 NOZ platí: *„je-li ujednána smluvní pokuta, nemá věřitel právo na náhradu škody vzniklé z porušení povinnosti, ke kterému se smluvní pokuta vztahuje.“* Je-li tedy smluvní pokuta ujednána, představuje v podstatě paušalizovanou výši náhrady škody. Věřitel nemusí dokazovat výši vzniklé škody ani příčinnou souvislost mezi porušením povinnosti a vzniklou škodou (jako by tomu bylo v případě uplatnění nároku na náhradu škody), avšak není oprávněn požadovat náhradu škody, která sjednanou smluvní pokutu převyšuje. (Achour, Pelikán, 2015, s. 88)

  Ustanovení § 2050 NOZ však není ustanovením kogentním, tzn. lze se od něj smluvně odchýlit. V případě zájmu o nárok na smluvní pokutu i náhradu škody současně je nutné tento požadavek výslovně uvést ve smlouvě. (Achour, Pelikán, 2015, s. 88)

  Dalším zajímavým a pro poškozenou stranu nepříjemným faktem je, že nepřiměřeně vysokou smluvní pokutu může soud na návrh dlužníka snížit, a to *„až do výše škody vzniklé do doby rozhodnutí porušením té povinnosti, na kterou se vztahuje smluvní pokuta. K náhradě škody, vznikne-li na ni později právo, je poškozený oprávněn do výše smluvní pokuty“.* (§ 2051 NOZ) Dle § 588 NOZ navíc soud i bez návrhu přihlédne k neplatnosti právního jednání, které se zjevně příčí dobrým mravům. (Havlík, 2013)

  Dále, v případě vzniku nemajetkové újmy, která má být nahrazena zadostiučiněním, se tato povinnost dle § 2984 NOZ posoudí obdobně podle ustanovení o povinnosti nahradit škodu. Achour a Pelikán (2015, s. 89) proto doporučují formulovat ujednání o smluvní pokutě tak, aby vedle zaplacení smluvní pokuty umožňovalo náhradu škody, ale i odčinění případné jiné újmy.

  Se zaměstnancem může zaměstnavatel ujednat smluvní pokutu pouze v rámci konkurenční doložky.
- Informační povinnost – strany by se měly vzájemně informovat o úniku informací.

- Ujednání o zvláštní ochraně autorských práv – pokud se s autorskými právy nakládá nebo je k plnění smlouvy použito autorské dílo, např. počítačový program, je vhodné věnovat pozornost i této speciální ochraně.

V případě zajištění ochrany informací vůči zaměstnancům má zaměstnavatel možnost vydat **pracovní řád**. Ten slouží k úpravě práv a povinností jak zaměstnance, tak zaměstnavatele. Dle § 306 ZP je pracovní řád *„zvláštním druhem vnitřního předpisu, jež rozvádí ustanovení tohoto zákona, popřípadě zvláštních právních předpisů podle zvláštních podmínek u zaměstnavatele, pokud jde o povinnosti zaměstnavatele a zaměstnance vyplývající z pracovněprávních vztahů".*

Pracovní řád nesmí zakládat nové povinnosti zaměstnance. Povinnosti lze ujednat pouze v pracovní smlouvě nebo jiném smluvním ujednání. Pracovní řád tyto povinnosti pouze blíže specifikuje. (Veřejný ochránce práv, 2016)

S pracovním řádem je zaměstnavatel podle § 31 ZP povinen seznámit nové zaměstnance ještě před nástupem do zaměstnání. Stávající zaměstnance je zaměstnavatel povinen informovat o vydání, změně nebo zrušení nejpozději do 15 dnů. Dále, dle § 305 odst. 4, musí být vnitřní předpis všem zaměstnancům zaměstnavatele přístupný.

Následující text se věnuje takovým firemním informacím, které si z pohledu jejich ochrany zaslouží zvláštní pozornost. Dle předmětu ochrany je lze shrnout následovně:

- obchodní tajemství
- know-how
- důvěrné informace
- osobní údaje

3.4 Obchodní tajemství

Obchodní tajemství je nehmotný statek, jedná se o nedílnou součást obchodního závodu a je majetkem podnikatele. (Štenglová, 2005, s. 15)

NOZ definuje obchodní tajemství v § 504 následovně: *„obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení."*

Abychom mohli určité skutečnosti považovat za obchodní tajemství, je nezbytné, aby splňovaly všechny **zákonem dané pojmové znaky** současně, proto jsou detailněji popsány níže:

- Souvisí se závodem – dané skutečnosti se závodem souvisí natolik, že jsou pro podnikatele z hlediska podnikání relevantní.
- Konkurenčně významné – jedná se o tržně využitelné informace, které jeho vlastníkovi (podnikateli) vůči konkurenci poskytují nezanedbatelnou výhodu, protože konkurence je nezná, nebo k nim nemá přístup.

- Ocenitelné – skutečnosti jsou nehmotným statkem s hodnotou vyjádřitelnou penězi, jsou tedy zpeněžitelné či jinak hospodářsky využitelné.
- Určitelné – je možné je dostatečně a určitě identifikovat např. v dokumentaci.
- Utajené – nejsou běžně dostupné v příslušných obchodních kruzích, čímž jsou myšleny osoby, které jsou potenciálními nebo skutečnými konkurenty podnikatele (nebo osoby, které by jim takové skutečnosti mohly sdělit). Přesto, že je např. skutečnost známá vědecké veřejnosti, nemusí být známá v příslušných obchodních kruzích.
- Utajení je odpovídajícím způsobem zajišťováno jejich vlastníkem – odpovídajícím způsobem znamená přiměřeně povaze a hodnotě utajované skutečnosti. (Černá a kolektiv, 2016, s. 207) (Doleček, 2015)

Obchodním tajemstvím mohou být například databáze odběratelů a dodavatelů, marketingová strategie, vzorníky, technologický postup, návod, projektová dokumentace, problematika cenové politiky a kalkulace, technický výkres, vynález, autorské dílo apod. (Čada, 2014, s. 60) O obchodní tajemství se však nejedná v případě patentovaných vynálezů a chráněných užitných či průmyslových vzorů, protože ty jsou veřejně dostupné. (Černá a kolektiv, 2016, s. 207)

Nositelem práva k obchodnímu tajemství je podnikatel provozující obchodní závod. Je tedy v jeho zájmu své obchodní tajemství utajovat a patřičně chránit, jelikož se jedná o informace, které mu přinášejí významnou konkurenční výhodu. Provoz takového závodu však nutně předpokládá, že je svěří nebo jinak zpřístupní alespoň některým svým zaměstnancům ať už plně nebo v rozsahu, v jakém je to k plnění jejich povinností potřebné. Fakt, že obchodní tajemství svěří nebo jinak zpřístupní zaměstnanci nebo skupině zaměstnanců však ještě neznamená, že je jeho právo na obchodí tajemství dotčeno. Podnikatel však musí ve vztahu k zaměstnancům přijmout odpovídající opatření potřebná k utajení obchodního tajemství. (Štenglová, 2005, s. 45)

Zajištění efektivní ochrany obchodního tajemství bývá obtížné. Je proto více než vhodné nepodcenit smluvní ani fyzickou ochranu. (Jansa, Otevřel, 2014, s. 160)

Obchodní tajemství je **chráněno přímo ze zákona** NOZ, TZ a autorským zákonem, a to po celou dobu, kdy jsou naplněny všechny zákonné znaky. (Jasna, Otevřel, 2014. s. 160)

V první řadě je obchodní tajemství chráněno zákonem č. 89/2012, občanským zákoníkem (NOZ), kde jeho ochrana vyplývá z ochrany vlastnictví (§ 1040–1042) a ze zákazu nekalé soutěže. Za nekalou soutěž se podle § 2985 považuje *„jednání, jímž jednající jiné osobě neoprávněně sdělí, zpřístupní, pro sebe nebo pro jiného využije obchodní tajemství, které může být využito v soutěži a o němž se dověděl*

a) tím, že mu tajemství bylo svěřeno nebo jinak se stalo přístupným na základě jeho pracovního poměru k soutěžiteli nebo na základě jiného vztahu k němu, popřípadě v rámci výkonu funkce, k níž byl soudem nebo jiným orgánem povolán

b) nebo vlastním nebo cizím jednáním příčícím se zákonu". (Doleček, 2015)

Při porušení obchodního tajemství tedy podnikateli přísluší ochrana jako při nekalé soutěži. To znamená, že *„osoba, jejíž právo bylo nekalou soutěží ohroženo nebo porušeno, může proti rušiteli požadovat, aby se nekalé soutěže zdržel nebo aby odstranil závadný stav. Dále může požadovat přiměřené zadostiučinění, náhradu škody a vydání bezdůvodného obohacení“*. (Maisner, 2011, s. 134)

Obchodní tajemství je chráněno také TZ (§ 248). Zde při naplnění znaků nekalé soutěže a způsobení škody ve výši nejméně 50 000 Kč hrozí pachateli odnětí svobody až na tři léta, zákaz činnosti nebo propadnutí věci. S porušením obchodního tajemství může souviset i trestný čin zneužití informací v obchodním styku, jež upravuje § 255. (Jansa, Otevřel, 2014, s. 161)

Některé druhy informací mohou být chráněny nejen jako obchodní tajemství, ale i autorským zákonem, např. zdrojové kódy software. (Jansa, Otevřel, 2014, s. 161)

Dle Jansy a Otevřela (2014, s. 160) je dokazování škody v praxi těžko prokazatelné, proto doporučují smluvní ochranu obchodního tajemství. Ta je výhodná především proto, že je možné zde přesně formulovat obchodní tajemství, formy jeho porušení a sankce. (Jansa, Otevřel, 2014, s. 161)

Nelze opomenout fyzickou ochranu informací v podobě omezených přístupů na určitá pracoviště či do informačních systémů apod. Podle dřívějšího OZ byla vazba mezi materiální a smluvní ochranou ze zákona dokonce povinná. Vlastník takových informací musel projevit vůli tyto informace utajovat. To mohl učinit např. v interním předpise nebo patřičným označením utajovaných informací. Pokud tomu tak nebylo, nebylo možné se při vyzrazení takových informací dovolávat práva na ochranu obchodního tajemství. (Maisner, 2011, s. 133)

NOZ přichází s koncepcí ochrany zájmů vlastníka. To znamená, že z okolností musí být zřejmé, že utajení daných skutečností je v zájmu jejich vlastníka. Ten o tom již ale není povinen učinit formální projev vůle. (Černá a kolektiv, 2016, s. 209) Nicméně označení obchodního tajemství, zabezpečení jeho dostatečné fyzické ochrany či úpravu podmínek pro zacházení s takovými informacemi v pracovním řádu lze i přesto jedině doporučit.

Je potřeba si také uvědomit to, že pouhé ujednání smluvních stran označující určité informace za obchodní tajemství ještě neznamená, že se tyto údaje obchodním tajemstvím stanou, pokud tyto informace nenaplňují pojmové znaky obchodního tajemství definované v § 504 NOZ. (Čada, 2010, s. 77)

3.4.1 Konkurenční doložka

K ochraně obchodního tajemství **po skončení pracovního poměru** slouží především konkurenční doložka. Jde o dohodu, ve které se zaměstnanec zavazuje, že se po určitou dobu po skončení zaměstnání (maximálně 1 rok) zdrží výkonu výdělečné činnosti, která by byla shodná s předmětem činnosti zaměstnavatele nebo která by měla vůči němu soutěžní povahu. Zaměstnavatel se za to zavazuje zaměstnanci poskytnout přiměřené peněžité vyrovnání, nejméně však ve výši jedné poloviny průměrného měsíčního výdělku, za každý měsíc plnění závazku. (Bělina, 2014, s. 177)

V konkurenční doložce je možné sjednat smluvní pokutu, kterou je zaměstnanec zaměstnavateli povinen zaplatit, jestliže závazek poruší, tedy bez ohledu na vznik škody. Její výše musí být přiměřená povaze a významu činností zaměstnance. (ZP)

Konkurenční doložka musí být uzavřena písemně, a to kdykoliv během pracovního poměru. Může se jednat o součást pracovní smlouvy, samostatnou smlouvu nebo o dodatek k pracovní smlouvě. V případě, že byla sjednána zkušební doba, může být konkurenční doložka sjednána až po jejím uplynutí, jinak je dohoda neplatná. To může pro zaměstnavatele znamenat problém, pokud má obavy z úniku důležitých informací a know-how, které zaměstnanci poskytne již ve zkušební době. (Šimečková, 2008, s. 100)

Podle § 310 ZP není možné konkurenční doložku sjednat s každým zaměstnancem, ale pouze v případech, jestliže to je možné od zaměstnance spravedlivě požadovat s ohledem na povahu informací, poznatků, znalostí pracovních a technologických postupů, které získal v zaměstnání u zaměstnavatele a jejichž využití při zaměstnancově následné výdělečné činnosti by mohlo zaměstnavateli závažným způsobem ztížit jeho činnost. Konkurenční doložku lze tedy sjednat se zaměstnanci, kteří pracují s takovými informacemi, které zaměstnavatel aktivně ochraňuje, např. důvěrné informace o dodavatelích, obchodní tajemství, know-how. Pokud zaměstnanec s takovými informacemi nepracuje, byla by konkurenční doložka s ním uzavřená relativně neplatná. Z uvedeného je zřejmé, že se konkurenční doložka bude ve většině případu sjednávat s řídícími pracovníky. (Šimečková, 2008, s. 109)

Konkurenční doložku je možné sjednat i v dohodách konaných mimo pracovní poměr. Zde však existuje riziko, že by toto ujednání mohlo být soudem shledáno v rozporu s dobrými mravy, jelikož tyto pracovněprávní vztahy mají pouze doplňkový charakter a neposkytují zaměstnancům ani dostatečně velký výdělek, ani dostatečnou ochranu zaměstnání. (Valíčková, 2016)

V literatuře se objevuje více názorů na to, k jakému okamžiku poměřovat konkurenční činnost. Zda pouze k okamžiku uzavření konkurenční doložky, celé době trvání pracovního poměru zaměstnance nebo až ke dni jeho skončení. Většina autorů se shoduje na tom, že rozhodujícím okamžikem je skončení pracovního poměru, protože mnoho informací, které zaměstnanec za dobu trvání pracovního poměru získal, už nemusí být dále zaměstnavatelem využívány pro jeho podnikatelskou činnost. Další otázkou je, zda má větší váhu samotný fakt konkurování předmětu činnosti podnikatele nebo skutečná soutěžní povaha jednání zaměstnance. Předmět činnosti podnikatele je vždy zapsán v obchodním rejstříku, tento zápis však nemusí plně odrážet aktuální stav, protože podnikatel už např. nemusí některou činnost vykonávat. Dle Šimečkové by proto mělo být přihlédnuto hlavně ke skutečné možnosti poškodit zaměstnavatele soutěžním chováním zaměstnance. (Šimečková, 2008, s. 104)

Zákon umožňuje konkurenční doložku vypovědět ze strany zaměstnance v případě prodlení zaměstnavatele s vyplacením peněžitého vyrovnání. Možné je

také odstoupení zaměstnavatele, ale pouze za dobu trvání pracovního poměru. (Bělina, 2014, s. 177)

Podle Jansy a Otevřela je konkurenční doložka velmi zneužitelným institutem. Důvod spatřují zejména v tom, že je pro zaměstnavatele velmi obtížné prokázat (nebo se o tom vůbec dozvědět), že zaměstnanec poskytl důvěrné informace konkurenci, nebo že s konkurencí spolupracuje. Přesto i po tuto dobu musí zaměstnanci vyplácet peněžité vyrovnání. (2014, s. 91)

3.5 Know-how

V literatuře i praxi se často považují za synonyma pojmy obchodní tajemství a know-how. Obsah tohoto výrazu není v české právní terminologii jasně vymezen, jeho úpravu však můžeme nalézt v nařízení Komise EU 330/2010. To definuje know-how jako *„tajný, podstatný a identifikovaný celek praktických nepatentovaných informací, které jsou výsledkem zkušeností dodavatele a jsou jím otestovány“*.

Know-how má tedy následující tři znaky:

- Tajné – jako soubor informací není všeobecně známé ani snadno dostupné. Jednotlivé části však nutně zcela neznámé či nedosažitelné být nemusí.
- Podstatné – jedná se o informace podstatné a užitečné pro výrobu, vývoj, používání, prodej nebo další prodej smluvního zboží a služeb.
- Identifikovatelné – know-how musí být dostatečně rozsáhle a srozumitelně popsané a vhodnou formou zaznamenané, aby bylo možné ověřit, zda splňuje podmínku tajnosti a důležitosti. (Černá a kolektiv, 2016, s. 212) (Čada, 2014, s. 70)

Tab. 1 Srovnání zákonných znaků obchodního tajemství a know-how

Znak	Obchodní tajemství	Know-how
Identifikovatelné	√	√
Týká se závodu	√	
Podstatný význam		√
Konkurenčně významné	√	
Ocenitelné	√	
Utajené	√	√
Zajištěná ochrana	√	

Zdroj: Vlastní práce autorky podle zdroje Černá a kolektiv, 2016, s. 212

Z výše uvedených znaků know-how a obchodního tajemství vyplývá, že know-how je (z právního hlediska) chápáno šířeji, protože zahrnuje i takové skutečnosti, které se netýkají závodu, nemusí být konkurenčně významné a jejich majitel nemusí zabezpečovat jejich ochranu. Je však zřejmé, že know-how bude často splňovat i některé znaky obchodního tajemství. (Černá a kolektiv, 2016, s. 212) Zejména

v případech, kdy se bude jednat o natolik důležité informace, které firmě přináší konkurenční výhodu, budou jistě jejím majitelem i aktivně utajované. Pokud je bude chtít navíc smluvně chránit, je nutné takové informace i ocenit.

Za know-how můžeme považovat zejména výrobní postupy, receptury, technické informace a dokumentace k výrobě určitého výrobku, výsledky pokusů a zkoušek apod. Jedná se však také o znalosti, zkušenosti, schopnosti a zručnosti, ať už byly zachyceni písemně či nikoliv. Jsou to skutečnosti, které jeho majiteli umožňují vyrábět nebo obchodně poskytovat něco, co by jinak vyrábět nedokázal nebo mu umožňují výrobu efektivnější či přesnější. (Čada, 2014, s. 70)

Na rozdíl od obchodního tajemství, **know-how není chráněno přímo ze zákona**. Podnikatel má možnost využít pouze ochranu smluvní. Jak již bylo zmíněno výše, know-how může často splňovat podmínky obchodního tajemství, v takových případech mu samozřejmě přísluší ochrana obchodního tajemství. (Maisner, 2011, s. 138)

Tak jako není zákonem definováno samotné know-how, tak není definována ani podoba smlouvy o know-how. Jedná se o zvláštní smluvní typ a není nikde stanoveno, jak má taková smlouva vypadat. Existují však jisté podobnosti např. se smlouvou licenční. (Čada, 2010, s. 91)

Přesná specifikace know-how či vyčíslení jeho peněžité hodnoty může být dle Čady velmi problematické, mnohdy spíše nemožné. Know-how totiž vzniká kombinací a postupným zdokonalováním činností ve výrobě nebo při poskytování služeb. Jedná se (většinou) o dlouhodobý proces, na kterém se přímo či nepřímo podílejí osoby s různým oborovým zaměřením, s různými zkušenostmi a schopnostmi. Vymezení předmětu smlouvy však představuje jeden z nejdůležitějších článků smlouvy, jehož nepřesná nebo nepromyšlená formulace může oběma stranám způsobit řadu problémů. (2010, s. 83)

Z výše uvedeného je zřejmé, že smlouvy o know-how podléhají mnoha různým vlivům a jen stěží se hledají nějaká obecná pravidla či vzory, jako je tomu u běžnějších smluvních typů, např. smlouvy kupní či smlouvy o dílo, které jsou přesně definovány zákonem, konkrétně NOZ. Při uzavírání smluv o know-how jsou kladeny vyšší požadavky na důvěru partnerů a jejich technickou úroveň, případně na mezinárodní aspekty. (Čada, 2010, s. 93)

3.6 Důvěrné informace

Další skupinou chráněných informací jsou informace důvěrné. Tento pojem bývá také často mylně zaměňován s pojmem obchodní tajemství. Zákon definici důvěrných informací neposkytuje, to je ponecháno na smluvních stranách. (Čada, 2014, s. 65)

NOZ o důvěrných informacích hovoří v § 1730 následovně: *„Poskytnou-li si strany při jednání o smlouvě údaje a sdělení, má každá ze stran právo vést o nich záznamy, i když smlouva nebude uzavřena. Získá-li strana při jednání o smlouvě o druhé straně důvěrný údaj nebo sdělení, dbá, aby nebyly zneužity, nebo aby nedošlo*

k jejich prozrazení bez zákonného důvodu. Poruší-li tuto povinnost a obohatí-li se tím, vydá druhé straně to, oč se obohatila.“

Důvěrné informace jsou tedy **chráněny ze zákona** v rámci tzv. předsmluvní ochrany. Hlavním důvodem je ochrana informací v případech, kdy k uzavření smlouvy nakonec nedojde. Při jednání o smlouvě se totiž strany snaží o druhé smluvní straně zjistit co nejvíce informací, které jim pomohou k rozhodnutí, zda danou smlouvu uzavřít nebo ne. Často se jedná o obchodní tajemství či know-how. (Uklein, 2015)

Formulace je však natolik obecná, že dokazování případné škody může být velmi složité. Zákon totiž nestanovuje ani charakter takových informací a nově ani nutnost takové informace označit. Postačuje, že z prohlášení druhé strany nebo okolností jednání o smlouvě vyplývá, že dané informace nesmí být druhou stranou zneužity či prozrazeny. (Callaghan, 2015)

V případě, že jsou v rámci předsmluvních jednání předávány důvěrné a pro smluvní strany důležité informace, je **vhodné uzavřít smlouvu** o jejich ochraně, kde budou dané informace a způsob jejich ochrany blíže určeny. (Maisner, 2011, s. 143)

3.7 Osobní údaje

Zákon č. 101/2000 Sb., o ochraně osobních údajů (dále „ZoOOÚ“), definuje osobní údaje takto: *„Osobním údajem je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“ Subjektem údajů je dle tohoto zákona „fyzická osoba, k níž se osobní údaje vztahují“.*

Osobní údaje se dělí do následujících skupin:

- Identifikační – vyjadřují nějakou vlastnost či charakteristiku, kterou rozlišujeme u všech lidí patřících do určité skupiny a jejíž použití je formálně podporováno nebo vyžadováno. Jedná se o údaje, které slouží k určení totožnosti subjektu, a které se vyskytují v úředních záznamech, jde např. o rodné číslo, číslo sociálního pojištění, číslo občanského průkazu, datum narození, jméno a příjmení, státní občanství nebo také elektronický podpis či fotografii. Jedná se o nejpočetnější skupinu osobních údajů.
- Kontaktní – znalost těchto údajů umožňuje danou osobu kontaktovat, patří sem zejména telefonní číslo, korespondenční či e-mailová adresa.
- Popisné – jedná se o informace, které poskytují již komplexní obraz o fyzické osobě. Jsou to např. informace o původu, zvycích, chování, dosaženém vzdělání, informace o rodinných vztazích či majetkových poměrech, nebo také informace o výšce a váze člověka.
- Transakční – tyto údaje vznikají výhradně činností správce nebo zpracovatele, často jsou vytvářeny pomocí automatizovaného evidenčního systému. Může se jednat např. o datum vzniku a ukončení pracovního poměru, pracovní funkce

> nebo číslo evidenční karty. (Novák, 2014, s. 87) (Matoušová, Hejlík, 2008, s. 21)

Úřad pro ochranu osobních údajů (dále „ÚOOÚ“) ve své příručce pro podnikatele definuje osobní údaje následovně: *„Osobní údaje tvoří soubor jednotlivých informací, které umožňují rozlišit příslušné subjekty údajů od jiných subjektů a kontaktovat je nebo poměrně jednoduše s nimi kontakt navázat a činit o subjektech údajů závěry, které je možné z takových údajů vyvodit. Při zpracování jsou tyto údaje považovány za osobní, pokud je možné z nich odvodit jejich vztah k příslušnému subjektu údajů.“* (2011, s. 7)

Aby se tedy jednalo o osobní údaj, musí být možné na základě něj (nebo na základě skupiny údajů) **identifikovat nebo kontaktovat** subjekt údajů, tzn. jednu určitou osobu. K identifikaci osoby někdy stačí jediný údaj, v jiných případech je nutná kombinace dvou nebo více údajů, zejména jde o kombinaci údajů identifikačních s údaji popisnými a kontaktními. Některé informace totiž samy o sobě osobními údaji nejsou, ale stávají se jimi až v kombinaci s dalšími údaji. Je proto velmi důležité zohlednit kontext takových informací. (Novák, 2014, s. 87)

O osobní údaj se také nejedná v případě, kdy je k jeho zjištění potřeba nepřiměřené množství času, úsilí nebo materiálních prostředků. (Novák, 2014, s. 89)

ZoOOÚ v § 4 dále definuje následující pojmy:

- Správce osobních údajů – určuje účel a prostředky zpracování osobních údajů, provádí samotné zpracování a odpovídá za něj. Tím může pověřit zpracovatele.
- Zpracovatel – na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje.
- Zpracování osobních údajů – je *„jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace“.*
- Souhlas subjektu údajů – je *„svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“.*

Správce může zpracovávat osobní údaje pouze **se souhlasem subjektu údajů**. Ten musí být při udělení souhlasu informován o tom, pro jaký účel, jakému správci a na jak dlouhou dobu souhlas dává. (Bartík, Janečková, 2010, s. 145)

Souhlas se zpracováním osobních údajů je svým charakterem jednostranné právní jednání, proto je jeho zařazení do smluvního ujednání nevhodné. Souhlas se zpracováním osobních údajů nesmí být podmínkou, která by, v případě jeho neudělení, znemožňovala uzavření smluvního vztahu. (Novák, 2014, s. 125)

Zákon nestanovuje přímo formu takového souhlasu, musí však splňovat určité náležitosti: musí být učiněn svobodně, vážně, určitě a srozumitelně. Subjekt údajů musí být předem informován o účelu a rozsahu zpracovávaných informací a o tom,

kdo a jak dlouho bude jeho osobní údaje zpracovávat. Obecné prohlášení „Souhlasím se zpracováním svých osobních údajů dle zákona o ochraně osobních údajů“ je proto naprosto nevyhovující. (Novák, 2014, s. 125)

Správce musí být také po celou dobu zpracování schopen prokázat, že mu subjekt údajů ke zpracování svůj souhlas poskytl. Písemný souhlas se zde proto jeví jako nejvhodnější. Výslovnost souhlasu však zákon nepožaduje, může proto být učiněn i konkludentně, např. tím, že subjekt údajů dané údaje zpracovateli sám poskytne. (Janečková, Bartík, 2012)

Bez souhlasu subjektu údajů může správce osobní údaje zpracovávat pouze v případech uvedených v § 5 odst. 2 ZoOOÚ. Pro podnikatele jsou nejdůležitější tyto dvě výjimky:

- pokud provádí zpracování nezbytné pro dodržení právní povinnosti správce
- pokud je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů (Bartík, Janečková, 2010, s. 145)

Správce může zpracovávat pouze osobní údaje takového typu, obsahu a rozsahu, který je přiměřený účelu, pro který jsou zpracovávány. Osobní údaje by se měly ve firmách uchovávat pouze po takovou dobu, jež je nezbytná pro dosažení účelu, pro který byly shromážděny. (Ochrana osobních údajů: vybrané otázky, 2011, s. 18)

Mezi hlavní **povinnosti správce** patří zajištění bezpečnosti osobních údajů, tzn. zavedení vhodných technických opatření (např. omezený přístup, šifrovaný přenos) a organizačních opatření (např. interní předpis popisující zpracování osobních údajů či školení příslušných zaměstnanců) zajišťujících ochranu osobních údajů proti jejich zničení, ztrátě, úpravám, neoprávněnému sdělování a jiným formám nezákonného zpracování. Bezpečnostní opatření by měla záviset na prostředí, ve kterém jsou osobní údaje zpracovávány. (Ochrana osobních údajů: vybrané otázky, 2011, s. 23)

Povinnost mlčenlivosti o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, je dána ze zákona (ZoOOÚ, § 15) všem zaměstnancům správce nebo zpracovatele, ale i všem fyzickým osobám, které na základě smlouvy nebo zákonných povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

Správce má dále povinnost informovat ÚOOÚ o zamýšleném nebo již probíhajícím zpracování osobních údajů. Výjimky z oznamovací povinnosti jsou uvedeny v § 18 ZoOOÚ, jedná se např. o zpracování osobních údajů zaměstnanců pro personální a mzdové účely. (Bartík, Janečková, 2010, s. 153)

S osobními údaji se v podnicích setkáme na dvou místech, buďto jde o osobní údaje zaměstnanců nebo o osobní údaje zákazníků.

3.7.1 Osobní údaje zaměstnanců

Ochrana osobních údajů v pracovněprávních vztazích se řídí více právními předpisy, v první řadě ZoOOÚ, dále ZP, zákonem o zaměstnanosti a NOZ.

Zaměstnavatel je ze zákona povinen pro stanovené účely zpracovávat některé osobní údaje současných, minulých nebo budoucích zaměstnanců. (Ochrana osobních údajů: vybrané otázky, 2011, s. 37)

V případě osob ucházejících se o zaměstnání ve společnosti je možné požadovat identifikační a kontaktní údaje, dále informace o vzdělání, dovednostech a profesní historii. Po skončení výběrového řízení je nutné uchazeči, který ve výběrovém řízení neuspěl, veškeré dokumenty s jeho osobními údaji vrátit nebo je zničit (životopis, výsledky přijímacích testů apod.). V případě uchování osobních údajů pro budoucí výběrové řízení je již nutný souhlas uchazeče. (Ochrana osobních údajů na pracovišti, 2014, s. 4)

Při vzniku pracovního poměru je sepsána pracovní smlouva a založen zaměstnancův spis, do kterého se ukládají veškeré jeho dokumenty. Jedná se zejména o pracovní smlouvu a mzdový výměr, tzv. osobní dotazník, dále také informace o docházce, práci přesčas, pracovních úrazech, informace potřebné pro výpočet mzdy či platbu sociálního a zdravotního pojištění. (Bartík, Janečková, 2010, s. 149)

Součástí osobního spisu zaměstnance bývá často také jeho **fotografie**. Ta je dle ZoOOÚ považována za osobní údaj. Co se týká faktu, zda zaměstnavatel potřebuje ke zpracování takové fotografie souhlas zaměstnance či nikoliv, to záleží na účelu zpracování. Nejčastější důvody, kdy zaměstnavatel požaduje fotografii zaměstnance, jsou:

- Vystavení služebního průkazu – povinnost vydat služební průkaz je uložena pouze některým zaměstnavatelům podle zvláštních právních předpisů, jde zejména o státní zaměstnance. V těchto případech se jedná o zpracování ve smyslu § 5 odst. 2 písm. a) ZoOOÚ, tedy zpracování nezbytné pro dodržení právní povinnosti správce a k takovému zpracování zaměstnavatel nepotřebuje souhlas zaměstnance.
- Bezpečnostní důvod – především ve velkých podnicích, kde se zaměstnanci vzájemně neznají, může vystavení fotografie v interním systému sloužit k ochraně práv podnikatele. V tomto případě zaměstnavatel také nepotřebuje souhlas zaměstnance, takové zpracování však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. (§ 5 odst. 2 písm. e) ZoOOÚ)
- Zveřejnění fotografie na webových stránkách – jedná se možná o nejčastější důvod, proč zaměstnavatel vyžaduje od zaměstnance jeho fotografii. V takovém případě už ale zaměstnavatel potřebuje souhlas zaměstnance. Stejně tak v případě, kdy zaměstnavatel vytváří interní databázi svých zaměstnanců, pro kterou nemá důvod opírající se o zajištění bezpečnosti a ochrany práv. V těchto případech navíc zaměstnavatel nesmí zapomenout na oznamovací povinnosti vůči ÚOOÚ vyplývající z § 16 ZoOOÚ. (Janečková, Bartík, 2012)

Po skončení pracovního poměru mohou být osobní údaje zaměstnavatelem zpracovávány pouze v případech stanovených zákonem, tj. pro účely penzijního či zdravotního pojištění, daní, archivace nebo v případě soudního sporu. (Ochrana osobních údajů na pracovišti, 2014, s. 22)

Osobní údaje zaměstnanců mohou být přístupné pouze dvěma skupinám příjemců: zaměstnancům, kteří mají od zaměstnavatele výslovné oprávnění a jejichž náplní práce je zpracování takových dat (např. nadřízení, mzdová účetní), a externím subjektům na základě právního předpisu (např. kontrola bezpečnosti práce či finanční kontrola). (Ochrana osobních údajů na pracovišti, 2014, s. 13)

3.7.2 Osobní údaje zákazníků

Podnikatelé zpracovávají osobní údaje zákazníků především v souvislosti s plněním plynoucím ze smlouvy nebo za účelem nabídky svých výrobků a služeb.

Uzavírání smluv obecně vymezuje NOZ, případně zvláštní právní předpisy. Rozsah osobních údajů nezbytných pro uzavření smlouvy zde není definován, nesmí však být vyšší, než je nezbytné pro identifikaci zákazníka a plnění smlouvy. Pro identifikaci klienta (fyzické osoby) zpravidla stačí jméno a příjmení, adresa bydliště, případně datum narození. Je zřejmé, že se množství a charakter údajů bude lišit v závislosti na povaze a typu nabízených služeb. (Ochrana osobních údajů: vybrané otázky, 2011, s. 43)

Zpracování osobních údajů pro **marketingové účely** je již poněkud složitější. Každý podnikatel by chtěl dát svým potenciálním zákazníkům vědět o svých výrobcích či službách. Za velmi vhodný prostředek pro tyto účely lze označit direct marketing, umožňující přesné zacílení, personalizaci sdělení a rychlou interakci.

Nástroje direct marketingu lze rozdělit podle způsobu předávání sdělení následovně:

1. Elektronické obchodní sdělení – zde patří zejména e-mail (jak jednotlivě zaslané obchodní nabídky, tak hromadné e-maily a newslettery), fax a telefonické oslovení neboli telemarketing
2. Sdělení předávaná poštou – zde se může jednat jak o adresné zásilky pro konkrétní zákazníky, tak různé neadresné letákové akce (Karlíček, Král, 2011)

Zasílání **elektronického obchodního sdělení** je v dnešní době velmi využívaný způsob oslovení zákazníků. Jako nejvhodnější prostředek se často jeví e-mail, zvláště ten hromadný. Je levný, příprava není náročná a je možné takto oslovit velké množství lidí za velmi krátkou dobu. Velmi lákavě může působit i telefonické oslovování zákazníků. Na českém trhu je navíc možné zakoupit databáze kontaktů podle požadovaných kritérií, např. věk, obor či lokalita, obsahující jméno, telefonní číslo a e-mailovou adresu. (Mareš, 2010)

S šířením tzv. obchodního sdělení je však spojeno několik zákonných omezení a podmínek, které je potřeba splnit. Zákon obchodní sdělení definuje v § 2: *„obchodním sdělením jsou všechny formy sdělení, včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé či nepřímé podpoře zboží či služeb nebo*

image podniku osoby, která je podnikatelem nebo vykonává regulovanou činnost". V § 7 je stanoveno, že obchodní sdělení lze šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem, a to pouze s předchozím souhlasem adresátů, je zde tedy uplatněn tzv. opt-in princip. Elektronickými prostředky jsou dle tohoto zákona *„zejména síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy, telekomunikační koncová zařízení a elektronická pošta".* (Zákon č. 480/2004 Sb., o některých službách informační společnosti) Z výše uvedeného vyplývá, že tato omezení se vztahují jak na e-mailovou, tak na telefonickou komunikaci. (Často kladené otázky k zákonu č. 480/2004 Sb., o některých službách informační společnosti, 2004)

Souhlas se zpracováním osobních údajů musí být po celou dobu zpracování daných osobních údajů prokazatelný. Podle ÚOOÚ tedy není možné zasílat obchodní sdělení ani na kontakty nalezené ve veřejně dostupných seznamech, pokud k tomu subjekt údajů neudělil souhlas. Zákon se tak vztahuje i na běžnou činnost obchodních zástupců, v jejichž pracovní náplni je oslovování potenciálních zájemců, což se běžně děje prostřednictvím e-mailu či telefonicky. Mnoho podnikatelů se domnívá, že pokud se takové oslovování neděje hromadným způsobem, o obchodní sdělení ve smyslu zákona č. 480/2004 Sb., o některých službách informační společnosti (dále jen „ZIS") se nejedná. Platnost šíření obchodního sdělení však není podmíněna určitým množstvím takových odeslaných sdělení. Porušením zákona je i odeslání jediného nevyžádaného obchodního sdělení. (Často kladené otázky k zákonu č. 480/2004 Sb., 2013) (Bartík, Janečková, 2010, s. 184)

Zajímavé je, že panuje nejednotnost ohledně toho, zda je udělení souhlasu předem nutné i pro telemarketing. Podle Urbana (2004) stačí, když klient vysloví souhlas ihned na začátku hovoru, přičemž postačuje ústní forma. Poté je možné obchodní sdělení klientovi sdělit. Autor také doporučuje nahrávání takových hovorů a jejich archivaci, přičemž klient musí souhlasit i s těmito skutečnostmi. To znamená, že telemarketing podle něj funguje na tzv. opt-out principu. Podle jiných autorů však telemarketing funguje, stejně jako obchodní sdělení zaslané elektronickou poštou, na základě opt-in principu, tedy pouze s předchozím souhlasem subjektu údajů. (Často kladené otázky k zákonu č. 480/2004 Sb., 2004)

Bez souhlasu subjektu údajů lze dle zákona obchodní sdělení zasílat pouze zákazníkům, od kterých byl elektronický kontakt získán v souvislosti s prodejem výrobku nebo služby, a to pouze za předpokladu, že *„zákazník má jasnou a zřetelnou možnost jednoduchým způsobem, zdarma nebo na účet této fyzické nebo právnické osoby odmítnout souhlas s takovýmto využitím svého elektronického kontaktu i při zasílání každé jednotlivé zprávy, pokud původně toto využití neodmítl".* Nemusí se přitom jednat pouze o uzavřený smluvní vztah, dostačující je i jednání o jeho vzniku. (§ 7 odst. 3 ZIS)

Dle § 7 odst. 4 je dále zakázáno *„šíření obchodního sdělení elektronickou formou, pokud:*

1. *tato není zřetelně a jasně označena jako obchodní sdělení,*
2. *skrývá nebo utajuje totožnost odesílatele, jehož jménem se komunikace uskutečňuje, nebo*

3. *je zaslána bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem nadále zasílány". (Zákon č. 480/2004 Sb.)*

Zajímavé je, že zákon upravuje rozesílání obchodního sdělení pouze elektronickými prostředky, ale nevztahuje se na **letákové nebo poštovní kampaně**. (Polčák, 2007, s. 122) Zde je potřeba se řídit zákonem č. 40/1995 Sb., o provozování rozhlasového a televizního vysílání. K zaslání reklamy v listinné podobě není potřeba souhlas adresáta předem (jedná se tedy o opt-out princip), ale je zakázáno šíření nevyžádané reklamy, čímž se rozumí případ, kdy *„adresát dal předem jasně a srozumitelně najevo, že si nepřeje, aby vůči němu byla nevyžádaná reklama šířena".* (§ 2 odst. 1 písm. c) K tomu může sloužit i označení poštovní schránky nápisem „Nevhazovat reklamní letáky" apod. V souvislosti se ZoOOÚ je však patrné, že se výše zmíněné jedná pouze neadresných reklamních sdělení, jelikož sdělení adresované konkrétní osobě již předpokládá znalost jejích osobních údajů a ty je možné zpracovávat pouze s jejím souhlasem. A pokud účelem zpracování, ke kterému dala daná osoba správci souhlas, nebylo i zasílání reklamního sdělení, bylo by zaslání obchodní nabídky, byť v listinné podobě, porušením ZoOOÚ, konkrétně § 5 odst. 1 písm. f).

Jak ZIS, tak zákon o provozování rozhlasového a televizního vysílání, představuje veřejnoprávní ochranu před nevyžádanou reklamou. Existuje však i občanskoprávní úprava stanovující skutkovou podstatu „dotěrné obtěžování", kterou nalezneme v NOZ (§ 2986). Dále je potřeba mít na paměti i TZ, který v § 18 upravuje neoprávněné nakládání s osobními údaji.

3.8 Citlivé údaje

Osobní údaje, jež si zaslouží zvláštní pozornost, jsou citlivé údaje. ZoOOÚ je definuje v § 4b následovně: *„citlivým údajem je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů".*

Jelikož jsou tyto údaje zákonem taxativně určeny, je poměrně jednoduché citlivé údaje správně určit. (Matoušová, Hejlík, 2008, s. 26) Jde o informace v největší míře důvěrné a soukromé, které nejintenzivněji zasahují do soukromí. Porušení těchto práv může pro subjekt údajů představovat porušení základních lidských práv či diskriminaci. Proto je jejich **zpracování** podle směrnice 95/46/ES, až na výjimky, **zakázáno**. (Novák, 2014, s. 101)

Zpracování citlivých údajů se zvlášť věnuje i ZP v § 316 odst. 4, podle něhož zaměstnavatel nesmí vyžadovat od zaměstnance informace, které bezprostředně nesouvisejí s výkonem práce, zejména informace o sexuální orientaci, původu, členství v odborové organizaci a politických stranách nebo hnutích, příslušnosti

k církvi nebo náboženské společnosti. Informace o těhotenství, rodinných a majetkových poměrech a trestněprávní bezúhonnosti může zaměstnavatel požadovat pouze v případech, kdy je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený, nebo v případech, kdy to stanoví zákon nebo zvláštní právní předpis.

Dle Bartíka a Janečkové bývá v oblasti pracovněprávní nejvíce nejasností ohledně informací o zdravotním stavu a výpisu z rejstříku trestů. Výpis z rejstříku trestů, který dokládá beztrestnost, není citlivým osobním údajem. Stejně tak potvrzení lékaře nebo zdravotnického zařízení o tom, že zaměstnanec je nebo není schopen vykonávat danou práci, není považováno za citlivý údaj. Takové informace může zpracovávat pouze lékař. Výjimkou představuje zaměstnávání osob se změněnou zdravotní schopností, kdy povinnosti zaměstnavatelů vyplývají ze zvláštních právních předpisů. (2010, s. 151)

3.9 Nařízení EU o ochraně osobních údaj

Evropský parlament v dubnu 2016 schválil nové nařízení o ochraně osobních údajů označované jako GDPR neboli General Data Protection Regulation (dále jen „GDPR“). To vstoupí v platnost 25.5.2018 a nahradí dosavadní Směrnici 94/95 EC i český zákon č. 101/2000 Sb., o ochraně osobních údajů. Hlavním cílem je zvýšení ochrany osobních údajů občanů, rovnocenná vymahatelnost práva v celé EU, stejné sankce a mnohem těsnější spolupráce dozorových orgánů. (European Commission, 2017)

GDPR se týká všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data občanů EU, včetně společností a institucí mimo území EU, které působí na evropském trhu. (GDPR.cz, 2015)

Vznik GDPR reaguje na zastaralou dřívější směrnici. V době jejího vzniku totiž neexistovaly sociální sítě, cloudová úložiště ani řada dalších technologií. Tento nedostatek se snaží GDPR odstranit, avšak ani toto nové nařízení nestihne držet krok s neustálým technologickým pokrokem. Již teď se ví, že neupravuje problematiku tzv. internetu věcí či big data analýz. (GDPR.cz, 2015)

Řada základních definic se od stávající právní úpravy nijak zvlášť neliší, např. subjekt údajů, správce či zpracovatel. Definice osobních údajů je rozšířena o technické parametry jako e-mail, IP adresa nebo tzv. cookie v zařízení uživatele. (Radičová, Burian, 2016)

3.9.1 Práva subjektu údajů

Hlavním přínosem nového nařízení je **posílení práv fyzických osob** – subjektů údajů, kterým změny umožní lepší kontrolu nad jejich osobními údaji. Nařízení má zajistit větší transparentnost. Subjektům údajů by tak měly být snadno dostupné informace o tom, jak a v jakém rozsahu jsou jejich osobní údaje zpracovávány. (Radičová, Burian, 2016)

Nově je v zákoně zakotveno právo fyzické osob na to „být zapomenut“, pokud si již nadále nepřeje, aby byly její osobní údaje zpracovávány. Správce těchto osob-

ních údajů má pak povinnost informovat další správce, kteří tyto údaje zpracovávají, aby vymazali veškeré odkazy na dané osobní údaje či jejich kopie. (Radičová, Burian, 2016)

3.9.2 Povinnosti správců

Rozšíření práv subjektů údajů s sebou přináší **rozšíření povinností správců a zpracovatelů** osobních údajů. I když nařízení vstoupí v platnost až v květnu 2018, firmy by se dle názorů odborníků měly připravovat s předstihem. Již nyní by se měly zaměřit na datový audit, revizi smluv a implementaci organizačních, technických i procesních změn. (GDPR.cz, 2015)

Pravděpodobně nejdůležitější povinnosti, které takto správcům osobních údajů vznikají, jsou:

- Implementace technických a organizačních opatření zajišťujících nezbytnou ochranu osobních údajů.
- Vypracování posouzení vlivu na ochranu osobních údajů – toto bude nutné u tzv. vysoce rizikových zpracování uvedených v seznamu zveřejněném dozorovým úřadem.
- Jmenování pověřence pro ochranu osobních údajů – jeho hlavním úkolem by měla být kontrola zpracování osobních údajů v souladu s nařízením, školení pracovníků, provádění interních auditů a celkové řízení agendy interní ochrany dat. Odpovědnost za dodržování GDPR však tito pověřenci nenesou, ta zůstává na správcích a nově i zpracovatelích osobních údajů.
- Zavedení tzv. pseudonymizace osobních údajů – to znamená zpracování osobních údajů takovým způsobem, že již nemohou být přiřazeny konkrétnímu člověku bez použití dodatečných informací, které jsou chráněny proti opětovnému přiřazení k původním údajům a musí být uchovávány odděleně.
- Vedení záznamů o činnostech zpracování – obsahem budou v zásadě stejné informace, které již nyní musí správce sdělovat dozorovému orgánu (ÚOOÚ) v rámci oznamovací povinnosti.
- Konzultace s dozorovým orgánem před samotným zpracováním osobních údajů. (GDPR.cz, 2015) (Radičová, Burian, 2016)

Stejně jako podle současné právní úpravy, tak i podle GDPR, může správce osobní údaje zpracovávat pouze se souhlasem subjektu údajů. Ten musí být podle nového nařízení učiněn svobodně, musí být konkrétní, informovaný, jednoznačný a ničím nepodmíněný. Pokud společnost zpracovává osobní údaje, k jejichž zpracování získala souhlas dříve, autorka webové stránky GDPR.cz Eva Škorničková doporučuje audit takových souhlasů, aby každý byl v souladu s GDPR. Pokud některý souhlas nebude splňovat požadavky nového nařízení, je nutné o souhlas subjektu údajů požádat zpětně. Výjimky, kdy je možné osobní údaje zpracovávat i bez souhlasu subjektu údajů, zůstávají i v novém nařízení. (GDPR.cz, 2015)

Pro firmy toto nařízení přináší nejen nové povinnosti, ale také vyšší sankce za jejich porušení. Ty se mohou vyšplhat až na 20 000 000 EUR nebo 4 % z celkového ročního obratu společnosti (vyšší z obou možností) a budou záviset na mno-

ha faktorech, jako např. povaha, závažnost a délka porušování. Sankce plynoucí z aktuální právní normy činí maximálně 10 000 000 Kč. (Radičová, Burian, 2016) (European Commission, 2017)

4 Vlastní práce

Tato část diplomové práce se zabývá analýzou stávajícího stavu ochrany informací v konkrétní firmě působící v oblasti informačních technologií. Jelikož si daná společnost nepřeje být jmenována, bude v dalším textu použito fiktivní jméno „společnost ABC“.

4.1 Společnost ABC

Jedná se o poměrně mladou firmu, kterou založilo několik přátel s vizí, že budou vyvíjet unikátní cloudovou aplikaci, která jejím uživatelům umožní analyzovat jejich data, nacházet v nich do té doby neznámé souvislosti, a tím zefektivňovat podnikové procesy.

Dalším cílem bylo budovat firmu na principech „svobodné firmy“. Mezi hlavní znaky takové firmy patří demokratický přístup na všech úrovních, decentralizace řízení, transparentnost jak navenek, tak i uvnitř firmy a také zodpovědnost a důvěra. A právě důvěra se zde často promítá do určité benevolentnosti v oblasti ochrany informací a určení si jasných pravidel.

Společnost ABC je středně velkou firmou, která (stav k 1.4.2017) zaměstnává bezmála 40 osob na hlavní pracovní poměr a více než 20 brigádníků na základě dohody o provedení práce (dále jen „DPP“). Většina zaměstnanců se věnuje programátorské činnosti a vývoji aplikace, ostatní působí v oblasti marketingu, obchodu a také administrativy a financí.

4.2 Informace ve společnosti ABC

Na vývoji výsledného produktu se zde podílí mnoho odborníků z různých oblastí, jejichž jedinečné znalosti a zkušenosti tvoří know-how dané firmy. Mnoho skutečností bude jistě tvořit také obchodní tajemství, nabízí se např. zdrojové kódy, návrhy řešení, různé metodiky výpočtů a analýz, projektové dokumentace, strategické a marketingové plány, cenové kalkulace či databáze zákazníků. Všechny tyto informace pomáhají vytvářet unikátní aplikaci, která podniku poskytuje jedinečnou pozici na trhu. Vyzrazením takových informací by došlo k ohrožení či dokonce ke ztrátě konkurenční výhody, kterou si firma vybudovala.

Společnost pracuje také s mnoha informacemi svých klientů a obchodních partnerů. Aplikace, kterou společnost ABC vyvíjí, má více podob pro různé skupiny zákazníků. Pro účely této práce je důležité říci, že všechny varianty aplikace pracují s citlivými daty zákazníků, především s informacemi týkajícími se např. obratu, počtu zákazníků, různých kalkulací a logistických řešení, přehledu majetku či finančních ukazatelů.

Samozřejmě firma zpracovává i informace o svých zaměstnancích, jako je jméno, datum narození, místo bydliště či jejich mzdové ohodnocení aj.

Z výše uvedeného vyplývá, že společnost ABC pracuje s různými druhy citlivých dat, a to jak interních (vlastní know-how a obchodní tajemství, osobní údaje zaměstnanců), tak externích (know-how a obchodní tajemství zákazníků a obchodních partnerů, osobní údaje klientů i třetích stran). Ochrana informací zde proto bude hrát velmi významnou roli.

Přesto společnost ABC nedisponuje žádným vnitřním předpisem, který by pravidla ochrany informací ve společnosti upravoval.

V následujícím textu bude provedena analýza současného stavu ochrany informací ve společnosti ABC. Nejdříve bude věnována pozornost ochraně důvěrných informací, obchodního tajemství a know-how, poté ochraně osobních údajů.

4.3 Ochrana důvěrných informací, obchodního tajemství a know-how ve společnosti ABC

Následující text se věnuje analýze stávajícího stavu ochrany důvěrných informací, obchodního tajemství a know-how ve společnosti ABC.

4.3.1 Ochrana vůči zaměstnancům

V rámci výkonu prací u společnosti ABC se zaměstnanci seznámí s množstvím informací, z nichž mnohé splňují znaky obchodního tajemství, know-how či důvěrných informací. Jedná se přitom nejen o informace týkající se přímo společnosti ABC, ale samozřejmě i jejích klientů a obchodních partnerů.

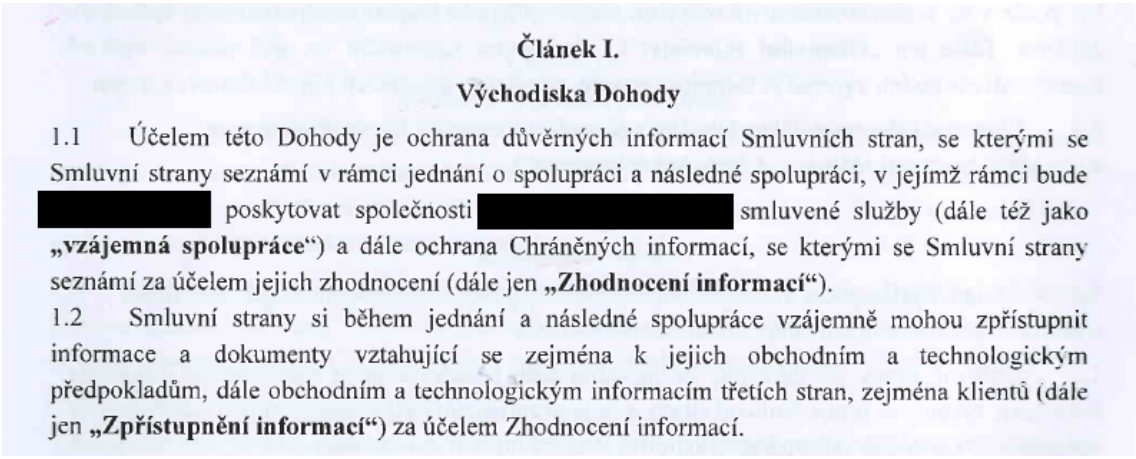
Ochrana takových informací je zajišťována různými fyzickými zabezpečeními a také smluvně. Každý zaměstnanec, který pracuje s cennými údaji, podepisuje tzv. NDA neboli dohodu o mlčenlivosti, ochraně informací a zákazu jejich zneužití (dále jen „dohoda o mlčenlivosti“). Společnost používá stejný vzor smlouvy, jako předkládá svým obchodním partnerům a klientům. Tento vzor si společnost ABC nechala zpracovat právnickou kanceláří asi před třemi lety. Znění smlouvy je stejné pro všechny zaměstnance, bez ohledu na funkci, pracovní náplň nebo rozsah informací, se kterými daný zaměstnanec pracuje. Ochrana informací a povinnost mlčenlivosti je částečně upravena také v pracovní smlouvě.

Fyzická ochrana je zajištěna v první řadě omezeným přístupem k elektronickým dokumentům pouze po zadání přístupového jména a hesla. Dokumenty v papírové podobě (smlouvy, objednávky, nabídky apod.) jsou uchovávány v policích ve společné kanceláři nebo na stolech či v zásuvkách jednotlivých zaměstnanců. Žádné z těchto dokumentů nejsou speciálně označeny např. jako „důvěrné informace“.

Zhodnocení stavu

Společnost ABC zvolila pro smluvní ochranu svých citlivých informací samostatnou smlouvu uzavíranou se zaměstnancem, což je v souladu se zákonem. Využívá však vzor smlouvy, který byl navržen pro ochranu informací vůči obchodním partnerům a klientům. Tento postup není vhodný, protože řeší i situace, které se zaměstnanců netýkají, a naopak některé aspekty jsou tak opomenuty. Dohoda o mlčenlivosti

upravuje vzájemné předávání dat většinou obchodního charakteru a jejich ochranu, přičemž je ale zřejmé, že zaměstnanec zde společnosti ABC žádné z uváděných dat zpřístupňovat nebude.



Článek I.

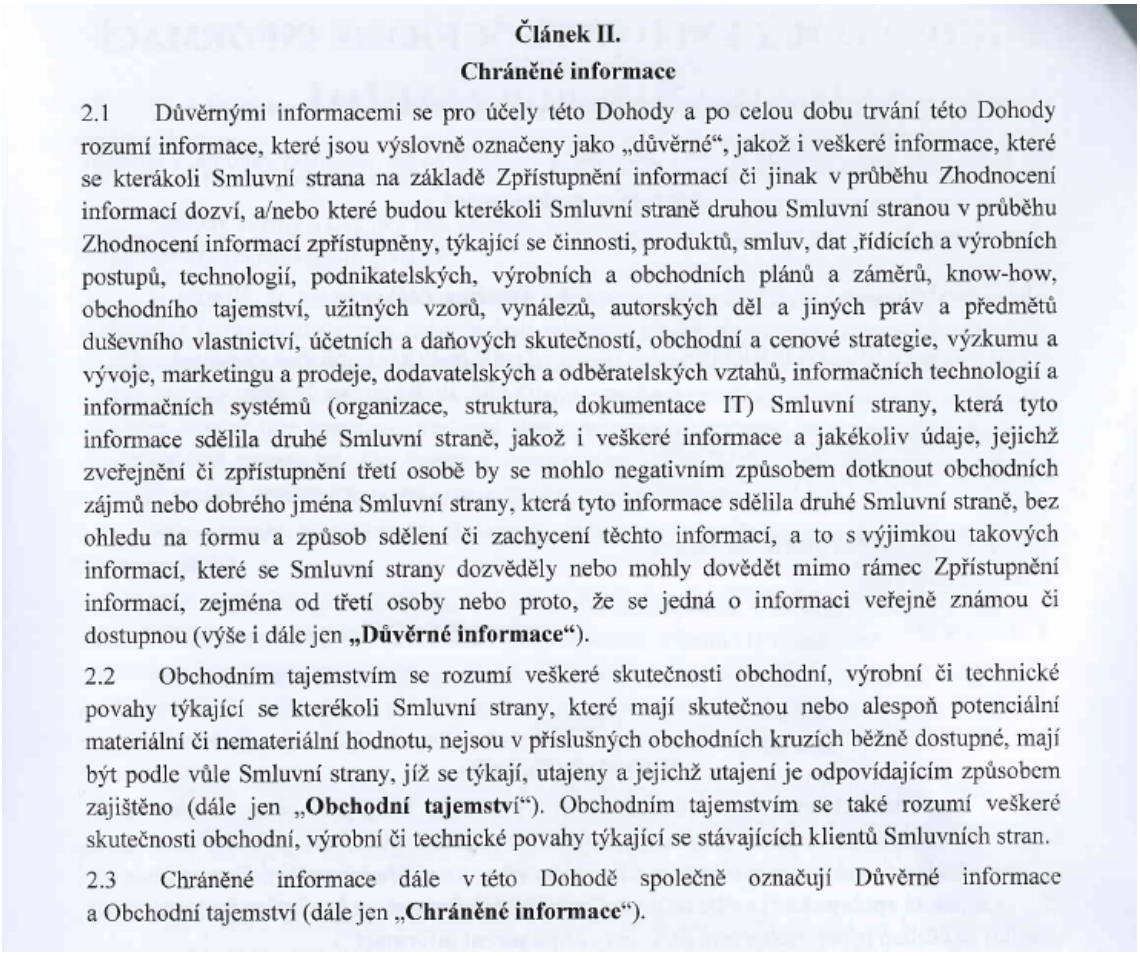
Východiska Dohody

1.1 Účelem této Dohody je ochrana důvěrných informací Smluvních stran, se kterými se Smluvní strany seznámí v rámci jednání o spolupráci a následné spolupráci, v jejímž rámci bude [redacted] poskytovat společnosti [redacted] smluvené služby (dále též jako **„vzájemná spolupráce“**) a dále ochrana Chráněných informací, se kterými se Smluvní strany seznámí za účelem jejich zhodnocení (dále jen **„Zhodnocení informací“**).

1.2 Smluvní strany si během jednání a následné spolupráce vzájemně mohou zpřístupnit informace a dokumenty vztahující se zejména k jejich obchodním a technologickým předpokladům, dále obchodním a technologickým informacím třetích stran, zejména klientů (dále jen **„Zpřístupnění informací“**) za účelem Zhodnocení informací.

Obr. 1 Dohoda o mlčenlivosti zaměstnance – východiska dohody
Zdroj: Smlouva společnosti ABC

Pro zajištění efektivní ochrany informací je naprosto klíčové správně a dostatečně **definovat chráněná data**. Společnost ABC v dohodě o mlčenlivosti definuje důvěrné informace a obchodní tajemství, jež společně označuje jako „chráněné informace“, viz obr. 2.



Článek II.

Chráněné informace

2.1 Důvěrnými informacemi se pro účely této Dohody a po celou dobu trvání této Dohody rozumí informace, které jsou výslovně označeny jako „důvěrné", jakož i veškeré informace, které se kterákoli Smluvní strana na základě Zpřístupnění informací či jinak v průběhu Zhodnocení informací dozví, a/nebo které budou kterékoli Smluvní straně druhou Smluvní stranou v průběhu Zhodnocení informací zpřístupněny, týkající se činnosti, produktů, smluv, dat ,řídících a výrobních postupů, technologií, podnikatelských, výrobních a obchodních plánů a záměrů, know-how, obchodního tajemství, užitných vzorů, vynálezů, autorských děl a jiných práv a předmětů duševního vlastnictví, účetních a daňových skutečností, obchodní a cenové strategie, výzkumu a vývoje, marketingu a prodeje, dodavatelských a odběratelských vztahů, informačních technologií a informačních systémů (organizace, struktura, dokumentace IT) Smluvní strany, která tyto informace sdělila druhé Smluvní straně, jakož i veškeré informace a jakékoliv údaje, jejichž zveřejnění či zpřístupnění třetí osobě by se mohlo negativním způsobem dotknout obchodních zájmů nebo dobrého jména Smluvní strany, která tyto informace sdělila druhé Smluvní straně, bez ohledu na formu a způsob sdělení či zachycení těchto informací, a to s výjimkou takových informací, které se Smluvní strany dozvěděly nebo mohly dovědět mimo rámec Zpřístupnění informací, zejména od třetí osoby nebo proto, že se jedná o informaci veřejně známou či dostupnou (výše i dále jen **„Důvěrné informace"**).

2.2 Obchodním tajemstvím se rozumí veškeré skutečnosti obchodní, výrobní či technické povahy týkající se kterékoli Smluvní strany, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle Smluvní strany, jíž se týkají, utajeny a jejichž utajení je odpovídajícím způsobem zajištěno (dále jen „**Obchodní tajemství**"). Obchodním tajemstvím se také rozumí veškeré skutečnosti obchodní, výrobní či technické povahy týkající se stávajících klientů Smluvních stran.

2.3 Chráněné informace dále v této Dohodě společně označují Důvěrné informace a Obchodní tajemství (dále jen „**Chráněné informace**").

Obr. 2 Dohoda o mlčenlivosti zaměstnance – definice chráněných informací
Zdroj: Smlouva společnosti ABC

Důvěrné informace takto definované zahrnují v podstatě všechny informace, které se zaměstnanec o společnosti ABC dozví, a to bez ohledu na skutečnost, zda jsou konkurenčně významné nebo způsobilé firmě způsobit újmu. Takovou povinnost mlčenlivosti není zaměstnanec schopen splnit a v případě soudního sporu by podle Jansy a Otevřela mohla být soudem posouzena jako protizákonná. (2014, s. 78) Definici důvěrných informací v této smlouvě proto považuji za příliš širokou a tedy nevhodnou.

Smlouva definuje také to, co se rozumí pod pojmem „obchodní tajemství". Aby se jednalo o obchodní tajemství podle § 504 NOZ a náležela mu tak i zákonná ochrana, musí splňovat všechny zákonem dané pojmové znaky současně: souvislost se závodem, konkurenční význam, ocenitelnost, určitelnost, utajenost a toto utajení je odpovídajícím způsobem zajišťováno jejich vlastníkem, tedy společností ABC. Informace, které tyto znaky nemají, nelze považovat za obchodní tajemství, a to ani v případě, že se na tom strany smluvně dohodnou.

Definice obchodního tajemství v dohodě o mlčenlivosti zcela opomíjí konkurenční význam informací. Podle ní by tak měly být chráněny i skutečnosti, jejichž

vyzrazení by nezpůsobilo újmu ani společnosti ABC, ani jejím klientům. Souvislost se závodem neznamená, že se údaje pouze týkají dané smluvní strany, ale že jsou pro podnik také významné. Dalším opomenutým znakem je ocenitelnost informací penězi a určitelnost informací.

Z výše zmíněného vyplývá, že obchodní tajemství definované v dohodě o mlčenlivosti není obchodním tajemstvím podle NOZ a nenáleží mu tak zákonná ochrana.

Obchodním tajemstvím se podle této dohody o mlčenlivosti rozumí také informace obchodní, výrobní a technické povahy o stávajících zákaznících společnosti. To však není možné, jelikož jedním ze zákonných pojmových znaků obchodního tajemství je souvislost s daným obchodním závodem, tedy se společností ABC. Ochranu takových informací proto navrhuji upravit v rámci ochrany důvěrných informací.

Společnost ABC využívá vzor dohody o mlčenlivosti určený pro použití ve vztahu k obchodním partnerům a klientům. Proto je zde i ujednání o **smluvní pokutě**. Smluvní pokutu může zaměstnavatel se zaměstnancem sjednat pouze v rámci konkurenční doložky. Toto ujednání je tedy v rozporu se zákonem.

4.2 V případě porušení povinností uložených článkem 3. odst. 3.3. této Dohody kteroukoli Smluvní stranou, má druhá Smluvní strana právo domáhat se vůči Smluvní straně, která povinnosti uložené článkem 3. odst. 3.3. této Dohody porušila, úhrady smluvní pokuty ve výši 250 000,- Kč (slovy: dvěstěpadesát tisíc korun českých).

Obr. 3 Smluvní pokuta v dohodě o mlčenlivosti zaměstnance
Zdroj: Smlouva společnosti ABC

Dále je zde sjednán **nárok na náhradu škody**. Ta poškozenému subjektu náleží ze zákona, avšak poškozená strana musí existenci a výši škody dokázat. V případě zaměstnance je navíc nutné zohlednit ZP. Pokud totiž došlo ke škodě způsobené porušením mlčenlivosti z nedbalosti, požadovaná částka náhrady škody může činit maximálně 4,5násobek jeho měsíční mzdy. V případě, kdy zaměstnanec způsobil škodu úmyslným porušením mlčenlivosti, zaměstnavatel může požadovat náhradu škody v plné výši, a navíc dokonce i náhradu ušlého zisku (§257 ZP).

4.4 Uplatněním nároku na úhradu smluvní pokuty či jejím uhrazením není dotčeno právo příslušné Smluvní strany na náhradu vzniklé škody. Pokud způsobená škoda přesahuje výši smluvní pokuty, má příslušná Smluvní strana právo domáhat se náhrady škody nad rámec smluvní pokuty.

Obr. 4 Náhrada škody v dohodě o mlčenlivosti zaměstnance
Zdroj: Smlouva společnosti ABC

Domnívám se, že v případě porušení mlčenlivosti zaměstnancem by se společnost ABC dostala do poměrně komplikované situace. Jednak by bylo vzhledem k nevyhovující definici „chráněných informací“ ve smlouvě obtížné dokázat vznik a výši způsobené škody, dále by bylo nutné přihlédnout ke skutečnosti, zda byla mlčenli-

vost porušena úmyslně nebo z nedbalosti, přičemž by podstatnou roli hrálo také to, zda byl **zaměstnanec o svých povinnostech dostatečně poučen**.

Podle § 31 ZP je totiž zaměstnavatel již před uzavřením pracovní smlouvy povinen seznámit uchazeče s právy a povinnostmi, které pro něj vyplývají nejen z pracovní smlouvy, ale také ze zvláštních právních předpisů vztahujících se k práci, která má být předmětem pracovního poměru.

Při nástupu do společnosti ABC nejsou zaměstnanci nijak zvlášť poučeni o charakteru chráněných informací ani o jejich ochranných opatřeních. Pouhé prostudování předložené dohody o mlčenlivosti, která nejenže obsahuje velmi obecné informace, ale navíc také ujednání v rozporu se zákonem, nelze dle mého názoru považovat za dostatečné splnění povinnosti zaměstnavatele podle § 31 ZP.

Dohoda nabývá **platnosti a účinnosti** dnem podpisu oprávněnými zástupci obou smluvních stran, doba účinnosti není stanovena. Jedno ze závěrečných ustanovení však upravuje vztahy po ukončení účinnosti této smlouvy, viz. obr. 5.

5.8 Závazky stanovené touto Smlouvou k ochraně skutečností tvořících obchodní tajemství a Důvěrné informace, které byly předány přede dnem ukončení účinnosti této smlouvy, platí i nadále po ukončení účinnosti této smlouvy, a to po dobu deseti let ode dne ukončení účinnosti této Smlouvy.

Obr. 5 Dohoda o mlčenlivosti zaměstnance – závazky po ukončení účinnosti smlouvy
Zdroj: Smlouva společnosti ABC

Z výše zmíněného není jasné, jak dlouho trvá zaměstnanci povinnost mlčenlivosti o chráněných informacích. Uzavřít smlouvu na neurčitou dobu s účinností do nekonečna, jak by šlo výše zmíněné ujednání chápat, je v podstatě možné. NOZ však v § 2000 poskytuje možnost domáhat se zrušení závazku, pokud smlouva zavazuje člověka na dobu delší deseti let. Stejně tak *„soud závazek zruší i tehdy, pokud se okolnosti, z nichž strany zřejmě vycházely při vzniku závazku, změnily do té míry, že na zavázané straně nelze rozumně požadovat, aby byla smlouvou dále vázána.“* Vzhledem k tomu, že mnoho informací se postupem času může stát všeobecně známými či pozbydou významu, jednalo by se o případ, kdy by soud závazek mlčenlivosti zaměstnance pravděpodobně zrušil.

Určité ujednání o mlčenlivosti zaměstnance obsahuje i **pracovní smlouva**. Sjednání povinnosti mlčenlivosti zaměstnance přímo v pracovní smlouvě zákon povoluje, stejně jako povoluje tuto povinnost sjednat v samostatné smlouvě či dodatku k pracovní smlouvě.

Ujednání v pracovní smlouvě, viz obr. 6, je však velmi obecné a plní funkci ochrany informací vůči zaměstnancům, kteří téměř vůbec nepřicházejí do styku s důvěrnými informacemi a není s nimi proto, dle společnosti ABC, potřeba podepisovat dohodu o mlčenlivosti. Ujednání není nijak v rozporu se zákonem, dle mého názoru je však nadbytečné, jelikož nestanovuje žádnou jinou povinnost než § 301 ZP, jež hovoří o řádném hospodaření s majetkem zaměstnavatele.

Oproti dohodě o mlčenlivosti je v pracovní smlouvě zmíněna povinnost zachovávat mlčenlivost o mzdových ujednáních mezi zaměstnancem a zaměstnavate-

lem a také to, že porušení mlčenlivosti představuje zvlášť hrubé porušení povinností zaměstnance, jež může být důvodem pro okamžité zrušení pracovního poměru zaměstnavatelem. Obě skutečnosti jsou v souladu se zákonem a lze pouze doporučit je do ujednání zahrnout.

IX.
Povinnost mlčenlivosti, použití informací, výkon jiné výdělečné činnosti

1. Zaměstnanec je povinen:
   a) zachovávat mlčenlivost o všech skutečnostech, o kterých se dozvěděl po dobu pracovního poměru a které v zájmu Zaměstnavatele nelze sdělovat jiným osobám;
   b) zachovávat mlčenlivost o všech skutečnostech, které tvoří předmět obchodního tajemství Zaměstnavatele;
   c) zachovávat mlčenlivost o veškerých mzdových ujednáních mezi Zaměstnancem a Zaměstnavatelem.

   Porušení povinnosti mlčenlivosti považují obě smluvní strany za zvlášť hrubé porušení povinností, které může být důvodem pro okamžité zrušení pracovního poměru podle ustanovení § 55 zákoníku práce.
2. Zaměstnanec se zavazuje, že nepoužije ve prospěch svůj či třetí osoby informace o skutečnostech, které se po dobu pracovního poměru dozvěděl, zejména obchodní kontakty, a to ani po skončení pracovního poměru.

Obr. 6 Povinnost mlčenlivosti zaměstnance v pracovní smlouvě
Zdroj: Smlouva společnosti ABC

Vzhledem ke všem výše zmíněným skutečnostem navrhuji odstranit nynější duplicitu úpravy povinnosti mlčenlivosti zároveň v pracovní smlouvě a v dohodě o mlčenlivosti. Společnosti navrhuji zvolit si jednu z následujících dvou možností:

- Povinnost mlčenlivosti upravit pouze v pracovní smlouvě (případně DPP) nebo pouze v dohodě o mlčenlivosti. Dle mého názoru je vhodnější pracovní smlouva (případně DPP), protože tak budou chráněny informace vůči všem zaměstnancům a není potřeba podepisovat další smlouvu. Pokud by, vzhledem k náplni práce jednotlivého zaměstnance, bylo nutné blíže specifikovat či rozšířit okruh informací, kterých se mlčenlivost má týkat, navrhuji upravit to v dodatku k pracovní smlouvě nebo v dohodě o mlčenlivosti. Jde však pouze o snížení administrativní náročnosti, z právního hlediska jsou obě varianty rovnocenné.
- Vytvořit pracovní řád, který bude detailně upravovat podmínky ochrany informací ve společnosti a k dodržování tohoto pracovního řádu zaměstnance zavázat v pracovní smlouvě (případně DPP). Tato varianta je dle mého názoru pro společnost ABC mnohem vhodnější, jelikož je závazná pro všechny zaměstnance a pracovní řád je možné ze strany zaměstnavatele kdykoliv jednostranně měnit. Je potřeba však pamatovat na to, že pracovní řád nesmí zaklá-

dat nové povinnosti zaměstnance. Povinnosti lze ujednat pouze v pracovní smlouvě nebo jiném smluvním ujednání. Pracovní řád tyto povinnosti pouze blíže specifikuje.

Návrh pracovního řádu pro společnost ABC upravující ochranu informací je uveden v příloze A. Samozřejmě může společnost v tomto dokumentu upravit mnohá další práva a povinnosti zaměstnanců i zaměstnavatele.

Ať už se společnost ABC rozhodne pro kteroukoliv z výše uvedených variant, kde povinnost mlčenlivosti stanovit, navrhuji tyto změny a doplnění oproti nynější úpravě:

1. Definice chráněných informací – smyslem je chránit pouze významné informace, nikoliv všechny informace. Definice by měla být proto prostá nejasností. Navrhuji následující znění:

„Zaměstnanci jsou povinni dodržovat mlčenlivost:

- *o všech informacích, které by mohly poškodit dobré jméno zaměstnavatele nebo mu způsobit materiální či jinou újmu;*
- *o všech důvěrných informacích, obchodním tajemství a o osobních údajích, se kterými se v rámci prací konaných u zaměstnavatele zaměstnanec seznámí, ať už se tyto informace týkají zaměstnavatele nebo jeho obchodních partnerů a zákazníků;*
- *o skutečnostech týkajících se bezpečnostních opatření chráněných informací.*

Pod pojmem obchodní tajemství se rozumí informace splňující současně všechny zákonné znaky definované v § 504 NOZ.

Pod pojmem osobní údaje se rozumí informace podle § 4 ZoOOÚ.

Pod pojmem důvěrné informace se rozumí:

- *jakékoliv informace, které zaměstnavatel výslovně označí jako „důvěrné informace“, přičemž se nejedná o nevyhnutelnou podmínku;*
- *neveřejné údaje o zákaznících zaměstnavatele, informace v obchodních nabídkách včetně ceny, projektové plány, analýzy, obsah obchodních smluv, historie e-mailové komunikace a zápisy z jednání s klienty, jakožto i jiné informace obchodní, výrobní či technické povahy, které se týkají zákazníků a obchodních partnerů zaměstnavatele;*
- *neveřejné informace o finanční a majetkové situaci zaměstnavatele, informace o marketingové a obchodní strategii, o projektech, plánech a záměrech zaměstnavatele, o jeho obchodních partnerech, klientech, obchodních a jiných kontaktech;*
- *informace o pracovních a výrobních postupech a metodách a jiném know-how zaměstnavatele;*
- *zdrojové kódy počítačových programů, bezpečnostní kódy a hesla;*

- *informace o mzdových podmínkách a jiných formách pracovního ohodnocení,*

a to bez ohledu na to, zda byly tyto informace zachyceny v písemné, ústní vizuální nebo elektronické podobě.

Zaměstnanci jsou dále povinni dodržovat veškerá bezpečnostní opatření nařízena zaměstnavatelem.“

2. Sankce – smluvní pokutu v NDA se zaměstnancem zákon nepovoluje, toto ujednání proto navrhuji ze smlouvy odstranit. Naopak doporučuji přidat následující:

„Porušení mlčenlivosti zaměstnance je závažným porušením jeho povinností, což opravňuje zaměstnavatele k okamžitému zrušení pracovního poměru podle § 55 ZP. Tím není dotčeno právo na náhradu škody ani ušlého zisku.“

3. Doba účinnosti – navrhují stanovit adekvátní dobu a tuto ve smlouvě srozumitelně definovat.

„Závazek mlčenlivosti zaměstnance platí po dobu existence chráněných informací, pokud tohoto závazku nebude zaměstnanec zaměstnavatelem dříve písemně zproštěn. Povinnost zachovávat mlčenlivost o chráněných informacích trvá i po skončení pracovního poměru zaměstnance ve společnosti ABC.“

V oblasti **fyzické ochrany informací** lze nalézt také několik pochybení. Ochrana dat v elektronické podobě je zabezpečena pomocí omezených přístupů pouze oprávněným osobám po zadání platného uživatelského jména a hesla. Toto opatření považuji za dostatečné, avšak doporučuji tuto ochranu nikdy nepodceňovat a jasně stanovit okruh oprávněných osob.

Dokumenty v papírové podobě jsou uloženy v polici ve společné kanceláři, k níž má přístup v podstatě kdokoliv. Společnost ABC tyto dokumenty neschovává v žádném uzamykatelném prostoru s přístupem pouze oprávněných osob, jelikož vychází z předpokladu, že všichni zaměstnanci podepsali dohodu o mlčenlivosti, jsou si vědomi své povinnosti zachovávat mlčenlivost a svým zaměstnancům v tomto ohledu velmi důvěřuje.

Může se zdát, že bezpečnostní opatření (ve fyzické i smluvní podobě) nejsou v prostředí plném důvěry potřeba. Avšak v případě prvního úniku cenných informací jistě každý změní názor. Kvalitní zabezpečení informací nejen zabraňuje jejich ztrátě, úniku či zneužití, ale také výrazně pomáhá při dokazování případné škody a poškozená strana, zde společnost ABC, může mnohem jednodušeji uplatnit svá práva na náhradu škody apod.

Doporučuji proto nepodceňovat ani fyzickou ochranu informací. Cenné dokumenty navrhuji uchovávat např. v uzamykatelné skříni s omezeným přístupem, nenechávat dokumenty volně ležet na stole nebo např. u tiskárny apod. Obzvláště

důležité dokumenty, ať už ve fyzické nebo elektronické podobě, navrhuji výslovně označit jako „důvěrné informace“. Toto zdánlivě nadbytečné opatření se však v případě zvláště cenných informací může jedině vyplatit.

Společnost má ještě jednu možnost, jak chránit své důvěrné informace vůči zaměstnancům, a tou je **konkurenční doložka**. Společnost ABC této možnosti za dobu své činnosti zatím nevyužila.

V konkurenční doložce se zaměstnanec zavazuje, že *„nejdéle rok po skončení zaměstnání nebude vykonávat výdělečnou činnost, která by byla shodná s předmětem činnosti zaměstnavatele nebo která by měla vůči zaměstnavateli soutěžní povahu“*. Nejde tedy jen o samotnou ochranu informací, která je ošetřena v pracovní smlouvě nebo v dohodě o mlčenlivosti, ale o závazek nevyužít chráněné informace při konkurenční činnosti. Konkurenční doložku je proto možné sepsat pouze se zaměstnanci, od nichž je spravedlivé takový závazek vzhledem k povaze informací, se kterými se ve firmě seznámí, požadovat. V případě společnosti ABC se jedná o zaměstnance na manažerských pozicích, kteří pracují s obchodním tajemstvím a důvěrnými informacemi společnosti, podílí se na tvorbě obchodní strategie společnosti a jsou s ní detailně seznámeni a využití těchto informací v následné konkurenční činnosti by společnosti ABC mohlo výrazně ztížit její činnost.

Přesto, že se konkurenční doložka jeví jako lákavý způsob ochrany podnikatelových informací, dle mnoha odborníků (Jansa, Otevřel, 2014) jde o značně zneužitelný institut. Prokázání škody a skutečnosti, že bývalý zaměstnanec zneužil informace ve prospěch konkurence, je značně obtížné. Zřejmě i z tohoto důvodu zůstává konkurenční doložka nevyužívaná i ve společnosti ABC.

Doporučení pro společnost ABC

V oblasti ochrany důvěrných informací, obchodního tajemství a know-how společnosti ABC doporučuji:

- Povinnost mlčenlivosti zaměstnance upravit pouze v jednom dokumentu, přičemž za nejvhodnější považuji pracovní řád. Další možností je pracovní smlouva (příp. DPP) nebo dohoda o mlčenlivosti.
- Jasně definovat chráněné informace.
- Odstranit ujednání o smluvní pokutě.
- Sjednat, že porušení mlčenlivosti je závažným porušením povinností zaměstnance, což opravňuje zaměstnavatele k okamžitému zrušení pracovního poměru, čímž není dotčeno právo na náhradu škody ani ušlého zisku.
- Dobu, po kterou je zaměstnanec povinen zachovávat mlčenlivost, vázat na dobu existence daných chráněných informací, přičemž tato povinnost platí i po skončení pracovního poměru zaměstnance ve společnosti.
- Nepodceňovat fyzickou ochranu těchto informací.

4.3.2 Ochrana vůči klientům a obchodním partnerům

Tato část se věnuje analýze současného stavu ochrany důvěrných informací, know-how a obchodního tajemství společnosti ABC, které zpřístupňuje svým obchodním partnerům a klientům v rámci obchodní spolupráce.

Mnoho takových informací je poskytováno již ve fázi předsmluvních vyjednávání, jejichž cílem je návrh aplikace na míru zákazníkovi. Takové informace jsou zákonem definovány jako důvěrné informace podle § 1730 NOZ. Společnost ABC zde poskytuje bližší informace např. o metodice analýz, výpočtech a algoritmech využívaných v aplikaci apod. Své důvěrné informace společnost ABC poskytuje také svým dodavatelům, např. účetní firmě či finančním poradcům.

Důvěrné informace jsou chráněny ze zákona. Definice je však natolik obecná, že v podstatě neposkytuje adekvátní ochranu. Efektivní bezpečnost důvěrných informací je proto vhodné zajistit navíc smluvně.

S novými klienty, u nichž dochází ke zpřístupnění citlivých informací, se proto sepisuje NDA neboli dohoda o mlčenlivosti. Společnost ABC používá buďto svůj vzor dohody o mlčenlivosti, který byl už zmíněn výše a který využívá i jako vzor dohody o mlčenlivosti se svými zaměstnanci, nebo přijímá smlouvy předložené klienty. Druhá možnost je mnohem častější, protože větší např. retailové nebo bankovní společnosti, se kterými společnost ABC často spolupracuje, mají svá právní oddělení, která jim připravují smlouvy a jiné smlouvy podepisovat ani nechtějí. Společnost ABC je zde v pozici smluvní strany se slabší vyjednávací pozicí.

Dále je provedena analýza smluv společnosti ABC a smluv předložených klienty, a to z pohledu ochrany informací společnosti ABC. Upozorněno bude zvláště na chybná, sporná nebo pro společnost ABC nevýhodná ujednání.

Zhodnocení stavu

Ve většině analyzovaných smluv shledávám problém opět v **definici chráněných informací**. Ta je příliš široká a zahrnuje tak i informace, u nichž nelze spravedlivě jejich ochranu požadovat.

Definice nejčastěji obsahuje výčet všech informací, které se týkají smluvních stran a potenciálně by mohly být důležité. Většinou specifikované pouze jako takové, jež nejsou veřejně známé. Často je ale ignorována skutečnost, zda jsou informace konkurenčně významné, podstatné a zda je v zájmu jedné ze smluvních stran takové informace chránit. Nejčastěji zní definice důvěrných informací takto:

1. Předmětem této smlouvy je závazek smluvních stran zachovávat mlčenlivost o všech údajích obchodního, právního, finančního, výrobního, technického apod. charakteru, týkajících se druhé smluvní strany, se kterými byli účastníci této smlouvy seznámeni v rámci vzájemné spolupráce, nebo které získali nebo měli z titulu vzájemné spolupráce k dispozici, včetně informací, které se týkají minulých, současných nebo budoucích výzkumných, vývojových nebo podnikatelských aktivit, produktů, zákazníků, know-how, služeb a technických poznatků druhé strany, a které nejsou veřejnosti běžně dostupné.

Obr. 7 Nejčastější definice chráněných informací ve smlouvě s klientem
Zdroj: Smlouva společnosti ABC

Je pochopitelné, že společnosti chtějí chránit veškeré své citlivé údaje, proto je ve smlouvě raději definují šířeji. Je však nutné si uvědomit, že to s sebou přináší i určitá úskalí. Vymahatelnost náhrady škody nebo smluvní pokuty je v případě široce či neurčitě pojaté definice chráněných informací velmi složitá. V krajním

případě může soud takové ujednání prohlásit za protizákonné, a tedy částečně neplatné.

Jako naprosto nevhodnou hodnotím definici důvěrných informací na obrázku 8. Formulace obsahuje řadu nejasností a chyb, a dle mého názoru tedy obrovský prostor pro vznik případných nedorozumění a neshod.

2. DŮVĚRNÉ INFORMACE

2.1. Smluvní strany sjednávají, že za důvěrnou informaci považují veškeré písemně předané informace důvěrné povahy, elektronické údaje nebo skutečnosti jakéhokoli druhu, včetně informací obchodních, výrobních, organizačních, technických, know-how nebo jakákoli jiná práva duševního vlastnictví, data, dokumenty, osobní údaje o jakékoli osobě nebo jiné informace týkající se klientů či jiných smluvních partnerů Smluvních stran, zaměstnanců, vnitřní informace (zejména, ale nikoli výlučně skutečnosti, které tvoří obchodní tajemství dle ust. § 504 občanského zákoníku), jakož i veškeré další písemně zachycené informace získané před nebo po podepsání této Smlouvy týkající se jedné Smluvní strany, která druhá Smluvní strana získala v souvislosti se Spoluprací (dále jen „**Důvěrné informace**").

2.2. Za Důvěrné informace Smluvní strany **nepovažují** informace, které jsou:

2.2.1. veřejné známé nebo se v budoucnu stanou veřejně známé široké veřejnosti se všemi detaily prokazatelně jinak než porušením povinností obsažených v této Smlouvě,

2.2.2. Smluvní straně prokazatelně známé před datem účinnosti této Smlouvy bez jakékoli povinnost nakládat s nimi jako s důvěrnými,

2.2.3. které příslušná Smluvní strana legálně obdrží od třetí osoby, která není nikterak povinna s nimi nakládat jako s důvěrnými,

2.2.4. ke kterým příslušná Smluvní strana nezávisle dospěje, aniž by porušila jakýkoli právní předpis nebo ustanovení této Smlouvy.

Obr. 8 Nevyhovující definice chráněných informací ve smlouvě s klientem
Zdroj: Smlouva společnosti ABC

Navrhuji proto vždy jasně definovat, které informace jsou stranami považovány za chráněné a vyhnout se obecným, neurčitým či mnohovýznamovým pojmům, jež by mohly vést ke sporům. Dle Jansy a Otevřela (2014, s. 163) není vhodné taxativní vymezení chráněných informací. Definici je naopak vhodné doplnit o uvedení demonstrativních příkladů konkrétních informací. Návrh definice důvěrných informací zní takto:

„Důvěrnými informacemi se pro účely této smlouvy rozumí informace poskytnuté smluvní stranou druhé smluvní straně během spolupráce podle této dohody, které nejsou veřejně známé nebo dostupné a které představují pro danou smluvní stranu určitou hodnotu, poskytují jí výjimečné postavení na trhu, a tedy tvoří konkurenční výhodu oproti jiným soutěžitelům a jejichž vyzrazení by mohlo dané smluvní straně způsobit materiální a/nebo nemateriální újmu, tedy poškodit dobré jméno firmy a/nebo ohrozit získanou konkurenční výhodu.

Pokud nejsou obchodním tajemstvím podle § 504 občanského zákoníku, považují se za důvěrné informace zejména:

- *jakékoliv informace, které smluvní strana výslovně označí jako „důvěrné informace“, přičemž toto označení není nevyhnutelnou podmínkou;*
- *neveřejné údaje technického a výrobního charakteru, jako např. specifikace aplikace a návrhy řešení, popis funkcionalit aplikace, algoritmy, náčrty, plány, koncepce, projektové plány, analýzy, výsledky výzkumu a vývoje, metodiky a jiné know-how apod.;*
- *neveřejné údaje obchodního, finančního či marketingového charakteru, jako např. strategické, marketingové, finanční či obchodní plány a záměry, cenové kalkulace, smlouvy, analýzy a jiné dokumenty tvořící součást nabídky, informace o zákaznících a partnerech smluvních stran, zápisy ze společných jednání apod.;*
- *zdrojové kódy aplikace, vynálezy a jiné zákonem chráněné předměty duševního vlastnictví.“*

Dalším podstatným bodem je **stanovení konkrétních bezpečnostních opatření** a podmínek nakládání s chráněnými informacemi, jež se strany zavazují dodržovat. Ve smlouvách jsou tyto skutečnosti většinou poměrně obsáhle popsány, viz např. obr. 9.

1. Na základě výše uvedeného se smluvní strany zavazují:

a) neposkytnout důvěrné informace získané v písemné, elektronické či ústní formě třetí straně bez předchozího výslovného písemného souhlasu té strany, které se informace bezprostředně týká,

b) důvěrné informace nezneužít, nepoužít v rozporu s oprávněnými zájmy druhé smluvní strany ve prospěch svůj nebo třetích osob a přijmout dostatečná opatření, aby se předešlo nepovolanému užívání důvěrných informací třetí stranou bez předchozího výslovného písemného souhlasu příslušné smluvní strany,

c) poskytovat důvěrné informace výhradně pracovníkům, kteří se podílejí přímo na spolupráci a užití jejích výsledků, tyto informace nezbytně potřebují k účelům, které jsou v souladu s účelem spolupráce a vedou přímo ke splnění jejích cílů,

d) nekopírovat důvěrné informace ani jiným způsobem je nereprodukovat bez výslovného souhlasu smluvní strany, která je zpřístupnila, kromě užití pro konkrétní, smluvními stranami stanovenou, interní potřebu smluvních stran,

e) pokud mají informace, zpřístupněné některou ze stran straně druhé charakter údajů chráněných zákonem o ochraně osobních údajů, dodržovat povinnosti tímto zákonem stanovené,

Obr. 9 Ochrana chráněných informací ve smlouvě s klientem – nedostatečná definice
Zdroj: Smlouva společnosti ABC

V tomto ujednání ale chybí jedna podstatná náležitost, a to **výslovný závazek důvěrné informace chránit a utajovat**, a také přijmout a dodržovat určitá bezpečnostní opatření. Dále zde není zmíněno, že strany jsou oprávněny zpracovávat důvěrné informace pouze k účelu, ke kterému byly zpřístupněny. Z tohoto pohledu považuji za mnohem vhodnější ujednání na obrázku 10.

1. Každá ze smluvních stran se zavazuje zajistit, aby nedošlo k úniku, zveřejnění a šíření Důvěrných informací získaných od druhé smluvní strany, a zavazuje se chránit tajnost Důvěrných informací minimálně stejným způsobem, jakým chrání své obchodní tajemství, vždy však způsobem obvyklým pro ochranu obchodního tajemství.
2. Každá ze smluvních stran se zavazuje vynaložit maximální úsilí, které lze spravedlivě požadovat, aby tajnost Důvěrných informací druhé smluvní strany byla důsledně dodržována jejími zaměstnanci i osobami, které k plnění účelu Spolupráce použije.
3. Kterákoliv smluvní strana je oprávněna zpřístupnit třetí osobě Důvěrné informace druhé smluvní strany pouze s předchozím písemným či emailovým souhlasem této druhé smluvní strany a vždy jen v rozsahu nezbytně nutném pro naplnění účelu, pro který jsou Důvěrné informace třetí osobě zpřístupněny a je-li taková třetí osoba zavázána povinností mlčenlivosti.
4. Smluvní strana, která zpřístupnila Důvěrnou informaci třetí osobě, odpovídá za jednání této třetí osoby tak, jako by jednala sama, a to i v případě, že se taková třetí osoba zaváže při plnění provést určitou činnost samostatně.
5. Smluvní strany se zavazují, že Důvěrné informace získané od druhé smluvní strany použijí výlučně pro účely, ke kterým byly Důvěrné informace druhé straně sděleny.

Obr. 10 Ochrana chráněných informací ve smlouvě s klientem – vhodná definice

Podstatným rozdílem oproti dohodě o mlčenlivosti sjednané se zaměstnancem je sjednání **smluvní pokuty**, což je v tomto případě v souladu se zákonem. Výše smluvní pokuty se ve společnosti ABC určuje pro každý případ individuálně, nejčastěji se pohybuje v rozmezí 1 000 000–10 000 000 Kč. Určení této hodnoty se nekonzultuje s právníkem, ani neprobíhá nějaký zvláštní proces ohodnocení zpřístupněných informací pro každý jednotlivý případ. Částka je většinou stanovena s ohledem na předešlé případy podobného charakteru.

3.3. Smluvní strany se dohodly, že v případě jakéhokoli porušení této dohody ze strany Příjemce informací, jeho zaměstnance či další osoby, jejíž činnosti využil Příjemce informací k realizaci spolupráce smluvních stran, je Poskytovatel informací oprávněn vyúčtovat Příjemci informací smluvní pokutu ve výši 3.000.000 Kč (slovy třimiliony korun českých) za každý jednotlivý případ porušení povinnosti. Smluvní pokuta je splatná do 10 dnů ode dne doručení písemné výzvy k její úhradě Příjemci informací, a to na účet uvedený ve výzvě. Příjemce informací podpisem této dohody výslovně potvrzuje, že výše smluvní pokuty dohodnutá v tomto ustanovení této dohody je přiměřená a opodstatněná, a vzdává se práva domáhat se u soudu snížení případných smluvních pokut vyúčtovaných Poskytovatelem informací v souladu s tímto ustanovením dohody.

3.4. Ustanovením o smluvní pokutě v této dohodě není dotčeno právo Poskytovatele informací na náhradu veškeré majetkové i nemajetkové újmy, na niž má Poskytovatel informací nárok v plné výši vedle smluvní pokuty.

Obr. 11 Smluvní pokuta a náhrada škody ve smlouvě s klientem
Zdroj: Smlouva společnosti ABC

Sjednání smluvní pokuty je pro společnost výhodné, protože se váže pouze na skutečnost porušení mlčenlivosti, nikoli na vznik škody. Poškozený tedy nemusí dokazovat vznik škody, ke škodě dokonce nemusí ani dojít. Hodnota smluvní pokuty však musí být přiměřená hodnotě, charakteru a významu chráněných informací, protože *„nepřiměřeně vysokou smluvní pokutu může soud na návrh dlužníka snížit s přihlédnutím k hodnotě a významu zajišťované povinnosti až do výše škody vzniklé do doby rozhodnutí porušením té povinnosti, na kterou se vztahuje smluvní pokuta. K náhradě škody, vznikne-li na ni později právo, je poškozený oprávněn do výše*

smluvní pokuty.“ (§ 2051 NOZ) Navíc dle § 588 *„soud přihlédne i bez návrhu k neplatnosti právního jednání, které se zjevně příčí dobrým mravům“*. Z těchto dvou ujednání firmě hrozí velké riziko, pokud smluvní pokutu stanoví neúměrně.

Výše smluvní pokuty by proto měla být stanovena s ohledem na výši předpokládané škody a na hodnotu závazku, který zajišťuje. Při určování přiměřenosti smluvní pokuty soud přihlíží také k dalším okolnostem provázejícím smluvní vztah, zejména k důvodům, které ke sjednání dané smluvní pokuty vedly a k okolnostem, které je provázely. (Dohnal a kol., 2016, s. 177)

Samotný fakt, že smluvní pokuta je nepřiměřená, ještě neznamená, že se současně příčí dobrým mravům. Rozpor s dobrými mravy musí odůvodnit nějaká další skutečnost, např. zavazuje k zachování mlčenlivosti o informacích, jejichž ochranu nelze spravedlivě požadovat. Lze proto předpokládat, že za neplatnou soud smluvní pokutu prohlásí pouze v ojedinělých případech. Mnohem pravděpodobnějším rizikem je snížení smluvní pokuty na návrh dlužníka. (Tintěra, 2015, s. 151)

Pokud si společnost není jistá určením výše smluvní pokuty, navrhuji konzultovat danou věc s odborníkem ještě před podpisem dohody o mlčenlivosti se smluvním partnerem. Společnost se tak vyhne případným soudním sporům, snížení smluvní pokuty nebo dokonce jejímu zrušení.

Odstavec 3.3. na obrázku 11 dále stanovuje, že příjemce informací výslovně potvrzuje, že výše smluvní pokuty je přiměřená a vzdává se svého práva domáhat se u soudu jejího snížení. To by bylo možné za předpokladu, že § 2051 NOZ je dispozitivní normou a lze se od ní smluvně odchýlit. Literatura na tuto otázku ale neposkytuje jednoznačnou odpověď, převládá pouze názor, že takové ujednání je v rozporu se zákonem. Platnost těchto ujednání proto nelze v současném českém právu garantovat. (Tintěra, 2015, s. 159) (Lovětínský, 2017)

Další důležitou skutečností týkající se smluvní pokuty je určení, zda má strana nárok vedle smluvní pokuty také na náhradu škody. Odstavec 3.4 na obrázku 11 stanovuje, že ujednáním o smluvní pokutě není dotčeno právo poškozené strany na náhradu škody. Dle § 2050 NOZ věřitel při sjednání smluvní pokuty nárok na náhradu škody nemá, avšak jedná se o dispozitivní normu a je tedy možné se smluvně odchýlit. Toto ujednání je tedy nejen v souladu se zákonem, ale navíc je pro poškozenou stranu výhodné, jelikož jí poskytuje větší zajištění v případě porušení povinností druhé strany i v případě vzniku škody. Proto doporučuji toto ustanovení vždy výslovně do smlouvy uvést, např. takto:

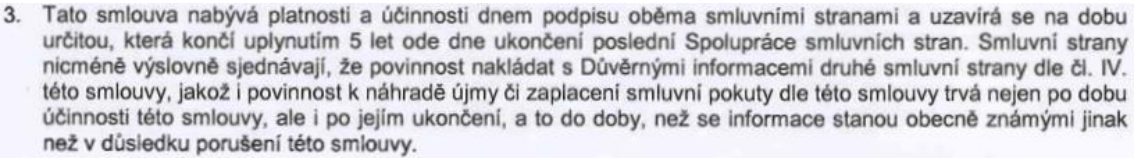
„Nárokem na smluvní pokutu není dotčen nárok na náhradu škody ani nárok na náhradu jiné (zejména nemajetkové) újmy v plné výši, tedy i ve výši přesahující smluvní pokutu.“

Doba účinnosti analyzovaných smluv byla většinou stanovena na dobu určitou, a to v rozmezí 3 až 10 let v závislosti na charakteru zpřístupněných informací v jednotlivých obchodních případech.

Nalezla jsem několik variant formulace doby účinnosti. Jako nejméně vhodnou hodnotím formulaci: „Tato smlouva nabývá platnosti a účinnosti dnem podpisu

oběma smluvními stranami a uzavírá se na dobu určitou, a to 5 let od podpisu této smlouvy.“ Toto ujednání je vhodné, pokud se nepočítá s delší spoluprací a předáváním zvlášť důležitých informací mezi smluvními stranami. Po uplynutí doby účinnosti smlouvy totiž zaniká povinnost mlčenlivosti a ochrany informací a také právo na smluvní pokutu či náhradu škody, a to pro společnost ABC hodnotím jako nevýhodné.

Dobu účinnosti smlouvy doporučuji formulovat s ohledem na délku spolupráce mezi smluvními stranami a dobu trvání závazku sjednat na dobu, po kterou budou mít informace znaky obchodního tajemství či důvěrných informací, a tedy hodnotu pro společnost ABC, viz obr. 12.



3. Tato smlouva nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami a uzavírá se na dobu určitou, která končí uplynutím 5 let ode dne ukončení poslední Spolupráce smluvních stran. Smluvní strany nicméně výslovně sjednávají, že povinnost nakládat s Důvěrnými informacemi druhé smluvní strany dle čl. IV. této smlouvy, jakož i povinnost k náhradě újmy či zaplacení smluvní pokuty dle této smlouvy trvá nejen po dobu účinnosti této smlouvy, ale i po jejím ukončení, a to do doby, než se informace stanou obecně známými jinak než v důsledku porušení této smlouvy.

Obr. 12 Platnost dohody o mlčenlivosti s klientem
Zdroj: Smlouva společnosti ABC

Výše byly shrnuty nejdůležitější náležitosti, které by měla dohoda o mlčenlivosti obsahovat, aby společnosti ABC zajistila efektivní ochranu důvěrných informací a usnadnila vymahatelnost v případě porušení povinností druhou smluvní stranou.

Dále lze doporučit ujednání upravující:

- Způsob sdělování informací – aby se předešlo nechtěnému zpřístupnění informací třetí straně, je vhodné upravit způsob komunikace smluvních stran. Mezi možnosti lze zařadit např. zakódovanou komunikaci, používání zvláštního softwaru pro přenos dat apod.
- Zvláštní ochranu autorských práv – pokud jsou mezi zpřístupněnými informacemi i autorské dílo či jiná práva duševního vlastnictví, je vhodné upravit ve smlouvě i jejich zvláštní ochranu. Proto dohoda o mlčenlivosti společnosti ABC obsahuje následující ujednání:

4.1. Poskytnutí či zpřístupnění chráněných informací nezakládá právo na licenci, ochrannou známku, patent, právo užití nebo šíření autorského díla, ani jakékoli jiné právo duševního nebo průmyslového vlastnictví. Chráněné informace, které mohou být zveřejněny Příjemcem informací postupem a v souladu s touto dohodou, nesmí obsahovat žádné údaje, záruky, jistiny nebo ručení, které by byly v rozporu s právy ochranných známek, patentovými právy, autorskými právy nebo dalšími právy duševního vlastnictví.

4.2. Veškeré chráněné informace, poskytnuté či zpřístupněné na základě této dohody, jsou a zůstanou vlastnictvím Poskytovatele informací a budou mu po ukončení smluvního vztahu založeného samostatně uzavřenými smlouvami, objednávkami či touto dohodou vráceny, pokud se smluvní strany v konkrétním případě nedohodnou jinak (např. skartace dokumentů).

Obr. 13 Ochrana autorských práv ve smlouvě s klientem
Zdroj: Smlouva společnosti ABC

- Informační povinnost – velmi vhodné je ve smlouvě upravit také povinnost informovat druhou stranu o již uskutečněném nebo jen hrozícím úniku informací. Smluvní strana, které se dané informace týkají, tak může přijmout dodatečná bezpečností opatření případně se připravit na hrozící rizika. Stejně tak lze doporučit sjednání možnosti požádat druhou smluvní stranu o prokázání plnění jejích povinností v oblasti ochrany informací. Takto může společnost kontrolovat, zda je s jejími informacemi nakládáno dle smlouvy.

Pokud by došlo k situaci, u které lze důvodně předpokládat ohrožení důvěrnosti Důvěrných informací, zavazuje se smluvní strana, u které tato situace nastala, oznámit tuto skutečnost bezodkladně druhé smluvní straně. Pokud by kterákoliv smluvní strana pojala důvodné podezření, že druhá smluvní strana není schopna zabezpečit ochranu Důvěrných informací dle této smlouvy, je oprávněna požádat tuto smluvní stranu o to, aby prokázala plnění povinností dle této smlouvy, a požádaná smluvní strana této žádosti vyhoví, oprávněné náklady s tím spojené však nese žádající smluvní strana.

Obr. 14 Informační povinnost ve smlouvě s klientem
Zdroj: Smlouva společnosti ABC

Doporučení pro společnost ABC

Výše byly shrnuty výsledky analýzy smluv zajišťující ochranu informací společnosti ABC vůči jejím klientům a obchodním partnerům. Doporučuji změny především v těchto oblastech:

- Jasná definice chráněných informací – doporučuji jasnou formulaci doplněnou o konkrétní příklady chráněných informací.
- Výslovný závazek dané informace chránit.
- Jasně definované podmínky práce s chráněnými informacemi a způsob jejich ochrany.
- Smluvní pokuta – navrhuji stanovit její výši s ohledem na hodnotu zajišťovaného závazku a výši možné škody.
- Výslovně stanovit, že nárokem na smluvní pokutu není dotčen nárok na náhradu škody ani nárok na náhradu jiné (zejména nemajetkové) újmy.

- Účinnost navrhuji sjednat s ohledem na délku spolupráce mezi smluvními stranami a dobu trvání povinnosti mlčenlivosti sjednat na dobu existence daných chráněných informací.

4.3.3 Ochrana důvěrných informací klientů a obchodních partnerů

V předcházející kapitole byla provedena analýza smluv z pohledu ochrany informací týkajících se společnosti ABC. Je však nutné si uvědomit, že dohoda o mlčenlivosti slouží k ochraně důvěrných informací obou smluvních stran, jimž takto vznikají nejen práva, ale i povinnosti.

Před podpisem dohody o mlčenlivosti je nutné zohlednit, že ujednání, která jsou pro společnost ABC výhodná z pohledu poskytovatele informací, pro ni nemusí být výhodná z pohledu jejich příjemce. Jakožto vlastník informací bude společnost požadovat co nejpřísnější ochranná opatření, jako příjemce naopak ocení co nejmenší množství povinností, nízké sankce apod. V následujícím textu bude upozorněno především na tyto odlišnosti.

V zájmu společnosti ABC, z pohledu příjemce informací, je především:

- Přesné označení chráněných informací – čím přesnější a jasnější je definice chráněných informací, tím menší je riziko vzniku nejasností a tím i potenciálního pochybení. V případě soudního sporu umožní jasná definice také účinnou obranu.
- Úzký okruh chráněných informací – v zájmu společnosti je závazek chránit a udržovat v tajnosti co nejmenší množství citlivých informací klientů a obchodních partnerů, jelikož s narůstajícím objemem chráněných informací je nutná větší kontrola a lze očekávat i narůstající prostor pro pochybení.
- Jasně definovaná bezpečnostní opatření – jasná definice opět zamezí vzniku pochybností a prostoru pro pochybení a v případě sporu umožňuje společnosti ABC lepší ochranu.
- Adekvátní sankce – při uzavírání dohody o mlčenlivosti je nutné zhodnotit, zda jsou navrhované sankce za případné porušení povinností plynoucích z dohody přiměřené, ale také jaké důsledky by případné uplatnění sankce pro společnost ABC mělo. Smluvní pokuta ve výši 10 mil. Kč by pro společnost ABC byla pravděpodobně likvidační. (Společnost v roce 2015 dosáhla tržeb 60 mil. Kč a zisku 2,2 mil. Kč, v roce 2016 tržeb 43 mil. Kč a ztráty 0,5 mil. Kč, hodnoty získány z účetní závěrky.)
- Sankce pouze za prokazatelné vyzrazení informací – doporučuji sjednat pouze sankce za prokazatelné porušení mlčenlivosti, nikoliv za jakékoliv porušení smlouvy, jak tomu ve většině analyzovaných smluv bylo. V krajním případě by tak společnosti hrozila sankce např. za neinformování zaměstnanců o povinnosti mlčenlivosti na základě dané smlouvy, přičemž v takovém případě je možné sjednat nápravu, aniž by druhá smluvní strana utrpěla nějakou újmu. (Jansa, Otevřel, 2014, s. 165)
- Smluvní pokuta vyjádřená fixní částkou – pro příjemce informací je výhodnější sjednání fixní smluvní pokuty než vyjádření např. procentem z obratu či jiné pohyblivé částky, jejíž vývoj lze do budoucna jen těžko predikovat.

- Sjednání smluvní pokuty a náhrady škody – pro příjemce informací je jistě výhodnější sjednání smluvní pokuty bez nároku na náhradu škody a/nebo nemajetkové újmy.
- Krátká doba trvání závazku mlčenlivosti – je pochopitelné, že pro zavázanou stranu je výhodnější co nejkratší doba, po kterou je povinna zachovávat mlčenlivost a dodržovat další povinnosti dané smlouvou. Z tohoto pohledu se jako výhodnější jeví stanovení doby trvání závazku na dobu určitou.
- Nevzdávat se dopředu práv – několik smluv předložených velkými společnostmi obsahovalo ujednání o tom, že se příjemce informací předem vzdává svého práva domáhat se u soudu snížení nepřiměřené smluvní pokuty. I když zatím neexistuje jednoznačný názor, zda je v tomto případě vzdání se tohoto práva v souladu se zákonem, přistoupení na takové podmínky považuji pro společnost ABC za nevýhodné.
- Ochrana práv obou smluvních stran – jelikož společnost ABC vystupuje v převážné většině vztahů spíše jako příjemce chráněných informací, může se zdát, že sjednávaná dohoda o mlčenlivosti je především v zájmu poskytovatele informací. V rámci spolupráce však vždy dochází k vzájemnému předávání informací, a i když jedna ze stran poskytne menší množství svých chráněných informací, neznamená to, že by neměly být chráněny. V rámci analýzy jsem se setkala se smlouvou, která upravovala vzájemné předávání informací, upravovala bezpečnostní opatření a povinnosti obou smluvních stran, avšak sankce za porušení mlčenlivosti plynula pouze společnosti ABC, v dané smlouvě označené jako „potenciální dodavatel“.

(e) Pokud *potenciální dodavatel* nebo některý z jeho *zástupců* z nedbalosti nebo vědomě poruší důvěrný charakter *důvěrných informací*, bude *potenciální dodavatel* povinen zaplatit [redacted] smluvní pokutu 25 tisíc EURO za každé porušení, které bude započteno na náhradu skutečné škody. Právo [redacted] na náhradu škody přesahující smluvní pokutu nebude zaplacením smluvní pokuty nijak dotčeno.

Obr. 15 Sankce pouze pro jednu smluvní stranu ve smlouvě s klientem
Zdroj: Smlouva společnosti ABC

Z výše uvedeného je zřejmé, že při vzájemném předávání informací dochází ke střetu zájmů dvou subjektů údajů. Smlouva by však neměla být pro jednu stranu výrazně méně výhodná, naopak by měla chránit zájmy obou smluvních stran. Společnosti ABC proto doporučuji věnovat pozornost ochraně jejích informací, nepodepisovat první verzi předložené smlouvy, pokud obsahuje pro ni nevýhodné podmínky, a snažit se vyjednat si podmínky lepší.

Dále doporučuji důsledně dodržovat povinnosti, které jí z dohody o mlčenlivosti plynou, např. mají-li být dokumenty uchovávány pouze na k tomu určených

datových nosičích nebo musí-li být označeny jako „důvěrné informace“ apod. Několik smluv obsahovalo také ujednání o povinnosti utajovat samotnou existenci dohody o mlčenlivosti a spolupráce daných smluvních stran. V případě, že je sjednána smluvní pokuta za porušení jakékoliv povinnosti plynoucí ze smlouvy, může i takové pochybení přijít společnost ABC draho, aniž by druhé smluvní straně způsobilo jakoukoliv újmu.

obě *strany* budou udržovat v tajnosti samotnou existenci této *Dohody*, její charakter i obsah, společně se skutečností, že probíhají nějaká jednání týkající se podnikání a souvisejících záležitostí *stran*.

Obr. 16 Povinnost zachovávat mlčenlivost o samotné existenci dohody o mlčenlivosti s klientem
Zdroj: Smlouva společnosti ABC

Ani ta nejlépe sepsaná smlouva však nezajistí účinnou ochranu informací. Toho může společnost dosáhnout pouze kombinací smluvní a fyzické ochrany. Jak již bylo zmíněno výše, nejslabším článkem je v oblasti ochrany informací lidský faktor. Zaměstnanci společnosti se mohou vědomě i nevědomě dopustit mnoha pochybení, která mohou mít v případě chráněných informací zákazníků a obchodních partnerů pro společnost ABC podstatné důsledky. Doporučuji proto pravidelně zaměstnance poučit o důležitosti takových informací a bezpečnostních opatřeních, která jsou povinni dodržovat.

4.4 Ochrana osobních údajů ve společnosti ABC

V předchozí části byla provedena analýza ochrany informací týkajících se společnosti ABC, které v zájmu zachování své konkurenční výhody chrání. Dále byla zpracována také analýza informací týkajících se klientů a obchodních partnerů, k jejichž ochraně se společnost ABC smlouvě zavázala. Nyní jde o skupinu informací, které je společnost ABC ze zákona povinna ochraňovat. Jedná se o osobní údaje.

Společnost ABC je správcem osobních údajů ve smyslu ZoOOÚ. Zpracovává osobní údaje svých zaměstnanců a osobní údaje zákazníků.

Níže je provedena detailní analýza současného stavu ochrany osobních údajů zaměstnanců a zákazníků ve společnosti ABC doplněná o návrhy řešení.

4.4.1 Osobní údaje zaměstnanců

Společnost ABC zpracovává řadu osobních údajů svých potenciálních, současných i bývalých zaměstnanců.

4.4.1.1 Osobní údaje uchazečů o zaměstnání

Společnost ABC své nové zaměstnance hledá vlastním úsilím. Nevyužívá tedy ani úřady práce ani personální agentury. Inzeráty zveřejňuje na svých webových stránkách a na vhodných internetových pracovních portálech.

V rámci výběrového řízení požaduje společnost ABC po uchazečích pouze strukturovaný životopis. Záleží na uchazeči, v jaké podobě životopis zašle a jaké informace zde o sobě uvede. Následně je uchazeč pozván na osobní pohovor, kterého se většinou účastní personalista a teamleader (vedoucí pracovník týmu, do kterého se uchazeč hlásí) a mnohdy také některý ze zaměstnanců, se kterým by uchazeč v případě přijetí úzce spolupracoval. Během výběrového řízení společnost o uchazečích získá množství osobních údajů, běžně se jedná o jméno a příjmení, datum narození, e-mailovou adresu, telefonní číslo a informace o dosaženém vzdělání a získaných zkušenostech. Životopis je v naprosté většině případů doplněn také fotografií kandidáta.

Společnost ABC si velmi zakládá na firemní kultuře a na dobrých vztazích mezi zaměstnanci, proto je pro ni důležité, aby každý nový člen do týmu „zapadl". O výběru vhodného kandidáta proto nerozhoduje pouze příslušný teamleader a personalista, ale i ostatní členové týmu, kteří s ním budou spolupracovat. Ti si mohou prohlédnout uchazečův životopis, dozví se řadu informací o jeho dovednostech a zkušenostech a následně se mohou zapojit do diskuse, zda tohoto kandidáta přijmout či nikoliv.

Po skončení výběrového řízení je běžnou praxí, že životopisy neúspěšných kandidátů bývají ve společnosti uchovávány. Většinou v elektronické podobě jako příloha e-mailu, který uchazeč dříve zaslal na personální oddělení nebo na společném cloudovém úložišti dat pro možné budoucí využití.

Zhodnocení stavu

Zaměstnavatel je oprávněn od uchazeče požadovat pouze takové osobní údaje, které bezprostředně souvisejí s obsazovaným pracovním místem a uzavřením pracovní smlouvy. (§ 30 ZP)

Z výše zmíněného lze vyvodit, že je naprosto v pořádku od uchazeče požadovat jméno, příjmení, kontaktní adresu, e-mailovou adresu nebo telefonní číslo. Toto jsou informace, které společnost potřebuje k základní identifikaci a kontaktování uchazeče. Informace o dosaženém vzdělání a nabytých zkušenostech jsou také v pořádku, pokud tyto informace bezprostředně souvisí s obsazovaným místem. V případě data narození a fotografie by však měla společnost postupovat opatrněji, protože zde neexistuje zákonná povinnost uchazeče tyto informace sdělovat. Navíc zde zaměstnavatel vždy musí brát ohled na riziko diskriminace. Tyto informace by tedy společnost neměla od uchazeče požadovat. Pokud však uchazeč sám dobrovolně o sobě sdělí informace důvěrného charakteru nebo informace nesouvisející přímo s obsazovaným místem, o porušení zákona se nejedná. Zaměstnavatel však tyto informace nesmí zpracovávat, tzn. ani uchovávat.

Další otázkou je **souhlas uchazeče se zpracováním osobních údajů**. Podle zákona o ochraně osobních údajů, může správce *„zpracovávat osobní údaje pouze se souhlasem subjektu údajů"*. V tomto případě se však uplatní výjimka, kdy je možné osobní údaje uchazeče zpracovávat i bez jeho souhlasu, definovaná v § 5 odst. 2 písm. b) ZoOOÚ, a to: *„jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů".* Zasláním životopisu do společnosti uchazeč

dává najevo, že má o nabízenou pracovní pozici zájem, tím pádem lze toto považovat za jednání o vzniku smlouvy uskutečněné na návrh subjektu údajů (uchazeče) a zaměstnavatel proto nepotřebuje výslovný souhlas se zpracováním jeho osobních údajů.

Zaměstnavatel je však oprávněn takové informace uchovávat pouze po dobu nezbytně nutnou k účelu jejich zpracování (§ 5 odst. 1 písm. e) ZoOOÚ). Účelem v případě výběrového řízení je obsazení inzerovaného pracovního místa nejvhodnějším kandidátem. Pokud tedy dojde k vybrání takového kandidáta, výběrové řízení tím končí a tím končí i účel, pro který je zaměstnavatel oprávněn uchovávat a zpracovávat osobní údaje ostatních uchazečů. Neúspěšným kandidátům je zaměstnavatel povinen vrátit poskytnuté dokumenty obsahující jejich osobní údaje nebo tyto dokumenty zničit. Uchovávání takových dokumentů není v souladu se zákonem.

Pokud by společnost ABC chtěla pro budoucí využití uchovávat životopisy kandidátů, kteří v daném výběrovém řízení neuspěli, musela by od nich získat souhlas. Vyžádání takového souhlasu dává smysl, pokud zaměstnavatel v blízké době plánuje obsazovat stejné či podobné pracovní místo nebo místo, pro které má daný kandidát vhodné kvality.

To lze učinit už během pracovního pohovoru nebo lze o takový souhlas požádat v e-mailu, ve kterém zaměstnavatel zašle uchazečům výsledek výběrového řízení. Žádost o souhlas splňující veškeré zákonné náležitosti (účel, rozsah zpracovávaných informací, dobu, určení správce) může vypadat následovně:

„Pokud máte zájem, aby Vaše osobní údaje byly nadále zpracovávány společností ABC pro účely budoucích výběrových řízení, pošlete mi, prosím, Váš souhlas jako odpověď na tento e-mail. Vaše osobní údaje budou zpracovány pouze pro účely budoucích výběrových řízení po dobu 6 měsíců a pouze v rozsahu, v jakém jste své osobní údaje sám uvedl ve svém životopise a při pracovním pohovoru. V opačném případě budou veškeré dokumenty obsahující Vaše osobní údaje zničeny v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů.“

Doba, po kterou je možné tyto dokumenty uchovávat není zákonem přesně stanovena. Je však vhodné zvážit aktuálnost takových informací. Dá se očekávat, že již po několika měsících od zaslání životopisu do společnosti ABC dojde u dané osoby k mnoha změnám. Je pravděpodobné, že si kandidát najde jiné zaměstnání a o pracovní pozici ve firmě ABC již nebude mít zájem, případně dojde ke změnám v jeho dosaženém vzdělání, absolvovaných kurzech a získaných dovednostech a tím se stanou informace o něm neaktuální. Dle mého názoru proto nemá smysl takové dokumenty uchovávat déle než půl roku. Delší dobu vnímám jako nepřiměřenou a bezúčelnou. Bartík a Janečkové také doporučují uchovávat tyto informace maximálně 6 měsíců. (2010, s. 148)

Podle § 18 ZoOOÚ nemá zaměstnavatel při zpracování osobních údajů uchazečů o zaměstnání oznamovací povinnost vůči ÚOOÚ, protože se jedná o zpracování údajů potřebných k uplatnění práv a povinností vyplývajících ze zvláštního zá-

kona, konkrétně § 30 ZP. V případě uchovávání životopisů po skončení výběrového řízení již oznamovací povinnost vzniká.

Pokud se tedy společnost ABC rozhodne uchovávat životopisy a jiné dokumenty obsahující osobní údaje neúspěšných uchazečů i po skončení výběrového řízení, musí získat prokazatelný souhlas se zpracováním jejich osobních údajů a také uchazeče informovat o účelu, rozsahu a době tohoto zpracování. Dále musí oznámit ÚOOÚ, že takové informace zpracovává.

Další skutečností, kterou by měla společnost ABC zohlednit při nakládání s osobními údaji uchazečů, je **okruh osob**, které s těmito údaji budou pracovat. Podle ZoOOÚ nemohou s osobními údaji pracovat všichni zaměstnanci, ale pouze oprávněné osoby, tzn. zaměstnanci k tomu zaměstnavatelem pověřeni. S osobními údaji kandidátů by tedy neměli pracovat zaměstnanci, kteří k tomuto účelu nemají výslovné oprávnění zaměstnavatele. Skutečnost, že je životopis uchazeče zpřístupněn celému týmu, může být považováno za jednání v rozporu se zákonem.

Pokud by společnost ABC nadále chtěla takto postupovat, je nutné, aby všechny zaměstnance řádně poučila o tom, že se jedná o osobní údaje a o povinnost mlčenlivosti vyplývající z § 15 ZoOOÚ. Vhodné je učinit tak formou vnitřního předpisu, se kterým se musí každý zaměstnanec při nástupu do společnosti ABC prokazatelně seznámit.

Doporučení pro společnost ABC

V oblasti ochrany osobních údajů uchazečů o zaměstnání společnosti ABC doporučuji:

- Požadovat pouze informace, které bezprostředně souvisejí s obsazovaným pracovním místem a uzavřením pracovní smlouvy. Jiné informace nevyžadovat a nezpracovávat.
- Informace uchovávat jen do skončení výběrového řízení, po skončení výběrového řízení všechny dokumenty neúspěšným kandidátům vrátit nebo je zničit.
- Pokud chce společnost uchovávat informace o kandidátech po skončení výběrového řízení, musí k tomuto zpracování získat jejich souhlas a toto zpracování oznámit ÚOOÚ.
- Určit okruh oprávněných osob, které s těmito informacemi pracují a tyto zaměstnance řádně poučit o povinnosti mlčenlivosti a ochrany osobních údajů.

4.4.1.2 Osobní údaje stávajících zaměstnanců

Ve společnosti ABC pracují jak zaměstnanci na základě pracovní smlouvy, tak brigádníci na základě DPP. Na základě těchto smluvních vztahů zpracovává společnost ABC řadu osobních údajů.

Firma požaduje osobní údaje pro identifikaci, kontakt a pro plnění svých zákonných povinností. Tyto povinnosti spočívají ve výpočtu mzdy a odvodu sociálního a zdravotního pojištění.

Tyto informace firma od svých zaměstnanců získává prostřednictvím „osobního dotazníku“, který musí vyplnit každý nový zaměstnanec. Dále je s ním sepsána pracovní smlouva a mzdový výměr, případně DPP.

Originály těchto dokumentů jsou založeny v osobních spisech jednotlivých zaměstnanců. Ty jsou uloženy v šanonu tomu určeném a ten je umístěn ve skříňce s uzamykatelnými dvířky ve společné kanceláři (open space). Kopie dokumentů se uchovávají v elektronické podobě na cloudovém úložišti dat. Jak ke klíčům k této skřínce, tak ke kopiím v elektronické podobě, má přístup omezený, avšak ne malý počet zaměstnanců. S těmito dokumenty pracuje personalista, mzdová účetní a dále čtyři administrativní pracovníci, z nichž dva zde pracují na základě DPP. Do dokumentů nahlíží i vedoucí pracovníci jednotlivých týmů.

Společnost uchovává i některé osobní údaje svých zaměstnanců nad rámec zákonného minima. Jedná se např. o fotografii, výsledky osobnostních testů a krátkou zprávu o zálibách zaměstnance. Všechny tyto informace tvoří tzv. „osobní profil zaměstnance“, který je umístěn v interním systému přístupném všem zaměstnancům. Práce s těmito údaji vyplývá z firemní kultury společnosti ABC, která je pro ni velmi důležitá. Sdílení těchto informací přispívá k přátelským vztahům mezi zaměstnanci a k lepšímu fungování týmů. Tyto informace slouží pouze pro interní účely a noví zaměstnanci tyto kroky činí zcela dobrovolně.

Fotografie je uchovávána jednak pro interní účely (součást „osobního profilu zaměstnance“), ale také pro zveřejnění na webových stránkách společnosti.

Zhodnocení

Podle § 312 odst. 1 ZP je zaměstnavatel oprávněn vést osobní spis zaměstnance. Ten smí obsahovat pouze písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu. Zde společnost ABC postupuje v souladu se zákonem.

Do osobního spisu mohou podle § 312 odst. 2 ZP nahlížet pouze vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni a dále např. ÚOOÚ nebo orgán inspekce práce.

Podle § 13 ZoOOÚ je správce osobních údajů povinen přijmout taková **bezpečnostní 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 k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů“*.

Uchovávání osobních spisů zaměstnanců v uzamykatelné skřínce je přiměřeným řešením s ohledem na velikost a charakter firmy. Jeden sdílený klíč umístěný v nezabezpečené zásuvce stolu jednoho z administrativních pracovníků již představuje nedostatečné zabezpečení ochrany, jelikož takto nelze zajistit, aby nedošlo k neoprávněnému přístupu k osobním údajům. Navrhuji určit dvě osoby, které s těmito dokumenty pracují nejčastěji, a těm přidělit vlastní klíč, za který budou zodpovědné. Tyto osoby mohou na žádost dokumenty zpřístupnit zbývajícím oprávněným osobám, které s nimi pracují jen příležitostně (např. pomocný administrativní pracovník nebo teamleader). Dvě osoby navrhuji z důvodu zastupitelnosti.

Také v případě dokumentů uložených na cloudovém uložišti dat je nezbytné, aby byl zajištěn přístup pouze oprávněným osobám na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby. Pro přístup k těmto dokumen-

tům musí osoba zadat uživatelské jméno a heslo. Stávající zabezpečení proto považuji za dostatečné.

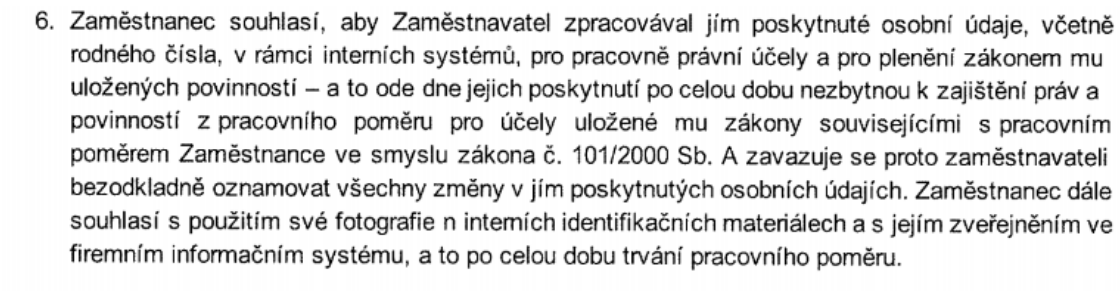
Podle § 5 odst. 2 ZoOOÚ společnost ABC nepotřebuje pro zpracování osobních údajů zaměstnanců jejich **souhlas**, jelikož *„provádí zpracování nezbytné pro dodržení právní povinnosti správce“*. Týká se to však pouze rozsahu nezbytně nutného pro plnění zákonných povinností zaměstnavatele.

Zpracování osobních údajů zaměstnanců pro plnění zákonných povinností zaměstnavatele nezakládá ani oznamovací povinnost vůči ÚOOÚ, jelikož se jedná o výjimku uvedenou v § 18 odst. 2 ZoOOÚ. V případě zpracování jakýchkoliv dalších osobních údajů už však oznamovací povinnost vzniká.

Z výše zmíněného vyplývá, že informace o zálibách zaměstnanců, výsledky osobnostních testů a fotografie nemůže společnost ABC od zaměstnanců požadovat a bez souhlasu je nemůže ani zpracovávat. Navíc zde společnosti ABC vzniká oznamovací povinnost vůči ÚOOÚ podle ZoOOÚ. Zde se nedá uplatnit žádná z výjimek uvedených v § 18.

Společnost ABC chtěla tuto situaci pravděpodobně vyřešit tak, že ujednání vyjadřující souhlas se zpracováním osobních údajů zaměstnanců vložila přímo do pracovní smlouvy, viz obr. 17. V tomto ujednání zaměstnanec uděluje souhlas se zpracováním svých osobních údajů pro plnění zákonných povinností zaměstnavatele, ale také souhlas s uveřejněním své fotografie v interním informačním systému. Toto ujednání je však chybné hned v několika ohledech:

- Pro zpracování osobních údajů zaměstnance za účelem plnění zákonných povinnosti zaměstnavatele není potřeba souhlas zaměstnance. Toto ujednání je ve smlouvě proto nadbytečné.
- Souhlas se zpracováním osobních údajů představuje jednostranné právní jednání a nemůže být proto součástí dvoustranného právního jednání, zde pracovní smlouvy. Stejně tak nemůže být uzavření pracovní smlouvy podmíněno udělením souhlasu se zpracováním osobních údajů. Z tohoto ohledu je ujednání v rozporu se zákonem.
- Společnost ABC využívá fotografii nejen pro interní účely, ale také pro zveřejnění na svých webových stránkách. Pro tento účel souhlas uvedený ve smlouvě nelze použít.



6. Zaměstnanec souhlasí, aby Zaměstnavatel zpracovával jím poskytnuté osobní údaje, včetně rodného čísla, v rámci interních systémů, pro pracovně právní účely a pro plenění zákonem mu uložených povinností – a to ode dne jejich poskytnutí po celou dobu nezbytnou k zajištění práv a povinností z pracovního poměru pro účely uložené mu zákony souvisejícími s pracovním poměrem Zaměstnance ve smyslu zákona č. 101/2000 Sb. A zavazuje se proto zaměstnavateli bezodkladně oznamovat všechny změny v jím poskytnutých osobních údajích. Zaměstnanec dále souhlasí s použitím své fotografie n interních identifikačních materiálech a s jejím zveřejněním ve firemním informačním systému, a to po celou dobu trvání pracovního poměru.

Obr. 17 Souhlas se zpracováním osobních údajů v pracovní smlouvě
Zdroj: Smlouva společnosti ABC

Informace, které společnost ABC potřebuje k plnění svých zákonných povinností, zjišťuje od nového zaměstnance prostřednictvím osobního dotazníku. Ten musí vyplnit každý nový zaměstnanec před sepsáním pracovní smlouvy. V tabulce níže jsou uvedeny **požadované údaje**, a dále zhodnocení, zda tyto údaje může podnik po zaměstnanci požadovat a účel, pro který mají být dané údaje zpracovávány.

Tab. 2 Osobní dotazník společnosti ABC

Položky v osobním dotazníku	Legálnost	Oprávněný důvod
Jméno a příjmení	√	Identifikace zaměstnance
Titul	√	Identifikace, potvrzení o dosaženém vzdělání, výpočet mzdy
Rodné příjmení	√	Sociální pojištění
Pohlaví	√	Sociální pojištění
Rodné číslo	√	Sociální a zdravotní pojištění, vyúčtování daně
Datum a místo narození	√	Zdravotní pojištění
Rodinný stav	√	Sociální pojištění a vyúčtování daně
Státní příslušnost, u cizinců také druh povoleného pobytu v ČR	√	Sociální pojištění
Číslo občanského průkazu nebo cestovního dokladu	Ano, ale	Přihlášení cizinců
Adresa trvalého bydliště	√	Sociální a zdravotní pojištění, vyúčtování daně, kontakt
Adresa přechodného bydliště	√	Kontakt, sociální pojištění
Číslo bankovního účtu pro účely výplaty mzdy (v případě zahraničního účtu se uvede IBAN a BIC/SWIFT	√	Výplata mzdy

kód)		
Zdravotní pojišťovna	√	Platba zdravotního pojištění
Počet dětí (u žen)	√	Sociální pojištění, vyúčtování daně
Druh a výše pobíraného důchodu	√	Sociální pojištění, vyúčtování daně

Zdroj: Interní dokument společnosti ABC

Z tabulky vyplývá, že společnost ABC v osobním dotazníku požaduje osobní údaje, které dle zákona požadovat může.

V případě občanského nebo cestovního průkazu požaduje správně pouze jeho číslo, nikoliv jeho kopii, protože to je na základě zákona č. 328/1999 Sb., o občanských průkazech a zákona č. 329/1999 Sb., o cestovních dokladech bez prokazatelného souhlasu občana zakázáno. Čísla těchto dokladů však může zaměstnavatel požadovat pouze od cizinců, účelem je přihlášení osob s jiným než českým občanstvím k sociálnímu a zdravotnímu pojištění. Čísla občanských průkazů osob s českou státní příslušností může zaměstnavatel zpracovávat pouze s jejich výslovným souhlasem, neboť pro to nemá zákonný důvod.

Doporučení pro společnost ABC

V oblasti ochrany osobních údajů stávajících zaměstnanců doporučuji společnosti ABC zejména:

- Nepodceňovat fyzické zabezpečení osobních údajů – dokumenty uchovávat např. v uzamykatelné skříňce, přístup k elektronickým dokumentům umožnit pouze po zadání přístupového jména a hesla.
- Určit okruh osob oprávněných pracovat s osobními údaji zaměstnanců a ty řádně proškolit.
- Zpracovávat pouze informace, které společnost potřebuje k plnění svých zákonných povinností.
- Zpracování jakýchkoliv dalších informací (např. fotografií, informací o zálibách apod.) doporučuji pouze se souhlasem zaměstnance a toto zpracování oznámit ÚOOÚ.
- Souhlas se zpracováním osobních údajů odstranit z pracovní smlouvy.

4.4.1.3 Osobní údaje bývalých zaměstnanců

Po skončení pracovního poměru se celý osobní spis zaměstnance přesune do šanonu určeného k archivaci a je uchováván za stejných podmínek jako osobní spisy stávajících zaměstnanců.

E-mailová adresa je zrušena, pokud byla na webových stránkách společnosti zveřejněna fotografie a kontaktní údaje na danou osobu, jsou tyto údaje smazány.

Zhodnocení stavu

Účelem zpracování osobních údajů zaměstnanců zaměstnavatelem je vedení mzdové a personální agendy za trvání pracovního poměru. S ukončením pracovní-

ho poměru tedy tento účel pomine. Po skončení pracovního poměru je zaměstnavatel povinen **uchovávat pouze některé dokumenty** na základě zvláštních právních předpisů. Jedná se zejména o stejnopisy evidenčních listů, účetní podklady, záznamy o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a záznamy potřebné pro účely důchodového pojištění.

Dalším oprávněným účelem je uchování dokumentů v případě sporu se zaměstnancem, např. o určení neplatnosti výpovědi nebo povinnosti zaplatit práci přesčas. Pro tento účel je možné uchovávat pouze takové dokumenty, které zaměstnavateli umožní hájit svá práva. S ohledem na tříletou promlčecí lhůtu je možné považovat za přijatelnou dobu pro uchování takových dokumentů 4 roky. Pro uchování dokumentů pro tento účel není potřeba souhlas zaměstnance, stejně tak se na tyto dokumenty nevztahuje oznamovací povinnost vůči ÚOOÚ. (Škubal, Vejsada, 2013)

Ostatní dokumenty je zaměstnavatel povinen vrátit zaměstnanci nebo zničit ihned po skončení pracovního poměru.

V tomto ohledu je možné postup společnosti ABC považovat v rozporu se zákonem, jelikož uchovává některé údaje, k jejichž zpracování nemá oprávněný důvod. Po skončení pracovního poměru zaměstnance totiž nedochází k likvidaci či vrácení dokumentů, ale pouhému přesunu dokumentů do jiné složky.

Co se týká bezpečnostních opatření těchto údajů, zhodnocení a doporučení jsou shodná s doporučeními uvedenými v předešlé kapitole, jelikož ochrana je zde zajišťována identickým způsobem jako v případě osobních údajů stávajících zaměstnanců.

Doporučení pro společnost ABC

V oblasti ochrany bývalých zaměstnanců společnosti ABC doporučuji:

- Po skončení pracovního poměru veškeré dokumenty danému zaměstnanci vrátit nebo je zničit, s výjimkou těch, jejichž archivace je dána zvláštním právním předpisem.
- Určit okruh oprávněných osob a zajistit fyzickou ochranu jako v případě osobních údajů stávajících zaměstnanců.

4.4.2 Osobní údaje zákazníku ve společnosti ABC

Společnost ABC zpracovává také osobní údaje svých stávajících a potenciálních zákazníků. Osobní údaje se týkají buďto fyzické osoby jakožto konečného zákazníka nebo kontaktní osoby v případě, že je zákazníkem firma. Jedná se především o jméno a příjmení, titul, telefonní číslo, e-mailovou adresu, adresu trvalého bydliště případně korespondenční adresu, pozici ve společnosti a mnohdy také datum narození. Datum narození se využívá k zaslání přání nebo speciální nabídky k narozeninám, v případě zákazníka (fyzické soby) také k identifikaci ve smlouvě.

S osobními údaji zákazníků pracují zaměstnanci z oddělení obchodu, marketingu a administrativy.

Veškeré údaje o stávajících i potenciálních zákaznících jsou ve společnosti ABC evidovány v elektronické podobě v CRM systému. Do tohoto systému mají pří-

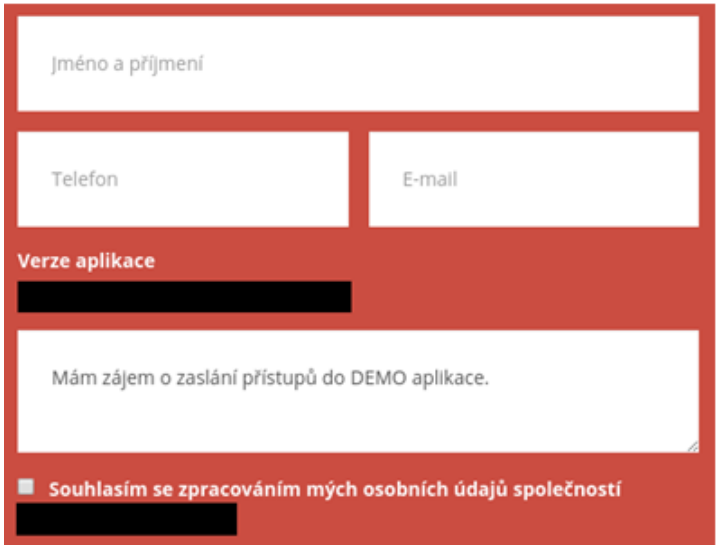
stup pouze oprávněné osoby, které s těmito informacemi pracují. Přístup do systému je možný po zadání uživatelského jména a hesla.

V případě zákazníků – fyzických osob – jsou osobní údaje uvedeny také ve smlouvě. Originál je uložen v příslušném šanonu v kanceláři ve volně přístupné polici. Kopie těchto smluv jsou uloženy na cloudovém úložišti dat, přičemž přístup k nim mají zaměstnanci, kteří s těmito informacemi pracují.

Údaje o svých stávajících klientech firma získává v průběhu obchodního jednání, při přípravě smlouvy a dále v rámci plnění ze smlouvy, zákaznického servisu a pro účetní účely. V případech, kdy nakonec z nějakého důvodu nedojde k podpisu smlouvy, získané informace společnost ABC dále eviduje.

Společnost ABC eviduje a zpracovává i osobní údaje potenciálních zákazníků, tedy osob, se kterými zatím žádný obchod uzavřen nebyl. Kontaktní údaje získává z několika zdrojů:

- Webové stránky společnosti – na webových stránkách společnost ABC uvádí kontakt přímo na své obchodní oddělení, dále je zde možnost vyplnit on-line kontaktní formulář v případě zájmu o konkrétní produkt či službu, e-book nebo demo verzi aplikace. Kontaktní formulář obsahuje možnost projevit souhlas se zpracováním osobních údajů společností ABC označením příslušného políčka křížkem, viz obr. 18.
- Doporučení – společnost získává kontakty také z doporučení od svých zákazníků či partnerů.
- Konference, veletrhy, školení – společnost se účastní oborově zaměřených akci, kde je možné nejen představit své produkty a služby, ale také získávat kontakty potenciálních zájemců.
- Vlastní vyhledání na internetu – společnost ABC vyhledává kontakty také sama na internetu. Vzhledem k účelu využití její aplikace je možné definovat určité okruhy firem, pro které by služby a produkty společnosti ABC mohly být zajímavé.



Obr. 18 Webový formulář společnosti ABC
Zdroj: Webová stránka společnosti ABC

Získané kontakty společnost ABC následně používá k oslovení těchto osob formou telefonního hovoru, hromadného e-mailu či dopisu. Stávajícím zákazníkům společnost pravidelně posílá elektronický newsletter s aktuální nabídkou či novinkami v aplikaci, mnohým klientům se posílá také přání k narozeninám.

Zhodnocení stavu

V některých oblastech ochrany osobních údajů zákazníků postupuje společnost ABC v rozporu se zákonem. **Fyzická ochrana** ve formě uchovávání informací ve speciálním CRM systému, ke kterému má přístup pouze omezený počet zaměstnanců a pouze po zadání správného uživatelského jména a hesla, můžeme považovat za dostatečnou ochranu. Uchovávání smluv ve volně přístupné polici v kanceláři již lze považovat za postup v rozporu se zákonem. Z § 13 ZoOOÚ společnosti ABC vyplývá povinnost *„přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě...“*, zde je však patrné, že společnost ABC taková opatření nepřijala.

Proto navrhuji přesné vymezení osob, které s těmito údaji pracují a přístup k dokumentům umožnit pouze těmto osobám. Smlouvy v papírové podobě navrhuji uchovávat v uzamykatelné, k tomu určené skříncе, přičemž klíč budou mít pouze tyto oprávněné osoby. Přístup k dokumentům v elektronické podobě by měl být umožněn pouze po zadání uživatelského jména a hesla.

Společnost ABC neplní řádně ani některé své povinnosti vyplývající z § 5 odst. 1 ZoOOÚ. Jedná se zejména o souhlas se zpracováním osobních údajů, účel, rozsah, přesnost a dobu zpracování.

Pro zpracování osobních údajů je nutný **souhlas subjektu údajů**. Výjimku tvoří zpracování osobních údajů *„nezbytné pro plnění smlouvy, jejíž smluvní stranou*

je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů" (§ 5 odst. 2 ZoOOÚ). Zpracovávat osobní údaje je dále možné pouze v souladu s účelem, k němuž byly shromážděny. Je proto nutné vždy účel stanovit.

Společnost ABC mylně ztotožňuje souhlas se zpracováním osobních údajů, jež upravuje ZoOOÚ, se souhlasem se zasíláním obchodních sdělení, který upravuje ZIS. Pokud tedy účel, pro který byly osobní údaje získány, nezahrnuje také zasílání obchodních sdělení, není možné tyto kontakty s obchodními nabídkami oslovovat. Zasílat obchodní sdělení lze také pouze se souhlasem daného subjektu. Bez souhlasu lze obchodní sdělení zasílat opět pouze stávajícím zákazníkům, ovšem ti musí mít vždy jasnou možnost bezplatně tento souhlas odmítnout. (§ 7 odst. 3 ZIS)

Společnost ABC v této oblasti opakovaně porušuje zákon tím, že využívá kontakty získané z on-line formulářů na svých webových stránkách k zasílání elektronického obchodního sdělení bez souhlasu těchto osob. Při vyplňování webového formuláře má osoba možnost pouze projevit souhlas se zpracováním svých osobních údajů (bez specifikace účelu, rozsahu a délky trvání), nikoliv však se zasíláním obchodního sdělení. Společnost ABC se zde mylně domnívá, že se jedná o výjimku podle § 7 odst. 3 ZIS. Osoby, které vyplní webový formulář, však nejsou zákazníky společnosti a neprojevují ani zájem o koupi výrobků a služeb společnosti ABC. Vyplněním formuláře osoba pouze projevuje zájem o zaslání e-booku, přístupových údajů do demo verze aplikace či se dozvědět o dané službě více.

Stejně tak je v rozporu se zákonem zasílání narozeninových přání nebo speciálních narozeninových nabídek osobám, pokud k tomu nedaly svůj souhlas. Účelem uvedení data narození ve smlouvě je totiž identifikace dané smluvní strany. Navíc je možné i obyčejné přání k narozeninám považovat za obchodní sdělení podle ZIS, jelikož slouží k podpoře image společnosti.

ZoOOÚ dále stanovuje, že *„subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období"*. Jednání společnosti lze v případě získávání kontaktních údajů na svých webových stránkách považovat za porušení zákona. Ze souhlasu se zpracováním osobních údajů, který zde uživatel může projevit, není patrný ani účel, rozsah a ani délka období. Patrné je pouze to, jakému správci osoba souhlas dává.

S ohledem na výše uvedené skutečnosti navrhuji změnit formulaci souhlasu se zpracováním osobních údajů v on-line formulářích a přidat možnost vyjádřit souhlas se zasíláním obchodního sdělení, přičemž bude možné vybrat každou možnost zvlášť pomocí označení zaškrtávacího pole. Formulace splňující veškeré zákonné náležitosti může znít např. takto:

- *„Souhlasím se zpracováním osobních údajů uvedených v tomto formuláři pro účely vyhotovení cenové nabídky a poskytnutí požadovaných služeb. Tyto údaje poskytuji pro výše uvedený účel zpracování společnosti ABC na dobu tří let od odeslání tohoto formuláře.*

- *Dále souhlasím se zasíláním obchodních sdělení společností ABC taktéž po dobu tří let od odeslání tohoto formuláře. Souhlas je možné kdykoliv odmítnout.“*

Shromažďování osobních údajů je navíc možné pouze v **rozsahu nezbytném pro stanovený účel**. Pro uzavření smlouvy jsou potřeba pouze údaje nutné pro identifikaci smluvní strany a plnění smlouvy. Pro potřeby společnosti ABC je z oblasti osobních údajů dostačující jméno a příjmení, adresa bydliště, případně datum na-rození. Dalším důležitým údajem je pochopitelně telefonní číslo a/nebo e-mailová adresa. Shromažďování jakýchkoliv dalších informací, které nejsou nutné k plnění smlouvy, k jejichž zpracování společnost ABC nedostala souhlas od daného subjektu údajů, již představuje porušení zákona. V případě společnosti ABC se jedná např. o informace o věku klientů.

Zákon dále stanovuje, že lze zpracovávat pouze **přesné osobní údaje** a je-li to nutné, je správce povinen osobní údaje aktualizovat. Společnost ABC však ve svém CRM systému eviduje velké množství osobních údajů, které vykazují zjevné nepřesnosti, jako např. překlepy ve jméně, chybně přiřazená e-mailová adresa nebo telefonní číslo ke konkrétní osobě. Nejčastější chybou je nepřesný název firmy včetně druhu obchodní společnosti. Mnoho kontaktů společnost získala již před delší dobou a nyní již nemůže zaručit aktuálnost nebo prokázat souhlas se zpracováním osobních údajů.

Společnosti ABC doporučuji věnovat pozornost bezchybnému zadávání kontaktů do svého CRM systému. Jména firem doporučuji uvádět v celém znění tak, jak jsou zapsána v obchodním či živnostenském rejstříku a staré údaje bez prokazatelného souhlasu vymazat.

Pochybení lze nalézt také v samotné podobě **obchodního sdělení** zasílaného elektronickou poštou. To musí být dle ZIS jasně a zřetelně jako obchodní sdělení označeno, musí obsahovat totožnost odesílatele a možnost se zdarma a jednoduše z odběru takových zpráv odhlásit.

Odhlášení se z odběru obchodních sdělení společnost ABC umožňuje pomocí odkazu pro odhlášení v patičce každého takového e-mailu, viz. obrázek č. 19. Totožnost odesílatele je v každé e-mailové zprávě zřetelně uvedena včetně kontaktu. Tato opatření považuji v souladu se zákonem.

Obr. 19 Odkaz pro odhlášení odběru obchodních sdělení společnosti ABC
Zdroj: E-mailoví obchodní nabídka společnosti ABC

Obchodní sdělení společnosti ABC však nejsou patřičně označena. Označení, že se jedná o obchodní sdělení, není umístěno v žádné části e-mailu, přitom ÚOOÚ upřesňuje: *„označení, že se jedná o obchodní sdělení, by mělo být umístěno v identifikačním poli zprávy“.* (Pavlát, 2013)

Velké pochybení ze strany společnosti ABC představuje **vyhledávání kontaktů na internetu** a následné oslovení těchto subjektů obchodními nabídkami. Spo-

lečnost ABC se domnívá, že pokud lze kontakt nalézt na internetu, je možné jej bez jakýchkoliv omezení také oslovit. Zde se společnost pravděpodobně opět dopouští jak poruše-ní ZIS, tak porušení ZoOOÚ. K zaslání obchodního sdělení elektronickou poštou ani ke zpracování jejich osobních údajů totiž tyto subjekty neudělily společnosti ABC souhlas. Zveřejnění kontaktních údajů zaměstnanců na webových stránkách obecně slouží výhradně k oslovení těchto osob s poptávkou po službách či produktech dané firmy, zaslání dotazu, vyřízení reklamace apod., nikoliv k zasílání obchodních nabídek.

Společnosti ABC proto doporučuji dále v tomto postupu nepokračovat a všechny kontakty, které takto získala, okamžitě smazat.

Dalšími způsoby, jak firma ABC získává kontakty na potenciální partnery či zákazníky, je **doporučení a různé konference či školení**, kde nejčastěji dochází k předání vizitek s kontaktními údaji. To lze vzhledem k účelu těchto akcí považovat za konkludentní vyjádření souhlasu se zpracováním osobních údajů i se zasíláním obchodního sdělení. Lze předpokládat, že osoba, která někomu předá svou vizitku s osobními údaji, ji předává za účelem zpracování údajů zde uvedených. Zasílat obchodní sdělení lze v těchto případech i na základě § 7 odst. 3 ZoOOÚ.

Komplikovanější je situace, kdy je kontakt získán z doporučení klienta či obchodního partnera. Může se zdát, že oslovení takové osoby je v naprostém pořádku, v obchodnické praxi je to velmi běžná situace a takové kontakty jsou mezi obchodníky navíc velmi ceněny. Zpracování těchto osobních údajů a následné zaslání obchodního sdělení je však v rozporu se zákonem, pokud k tomu subjekt údajů neudělil předem souhlas. Ten by navíc v takovém případě byl společností ABC těžko prokazatelný.

V situaci, kdy společnosti její stávající klient či obchodní partner doporučí kontakt na potenciálního zákazníka, doporučuji tohoto klienta či obchodního partnera požádat, aby předal kontakt na společnost ABC danému potenciálnímu zákazníkovi a aby on sám firmu kontaktoval. Tímto se společnost nedopustí porušení zákona a nepřijde ani o cenný obchodní kontakt. Oslovení společnosti ABC tímto potenciálním klientem je naprosto v souladu se zákonem.

Určitým řešením absence souhlasu se zasíláním obchodního sdělení by mohlo být **zasílání obchodního sdělení poštou**, protože zde nepotřebuje odesílatel souhlas předem. Muselo by se však jednat pouze o neadresnou nabídku. Tato varianta je vhodná spíše pro firmy nabízející produkty denní spotřeby nebo s cílením na velmi širokou cílovou skupinu. Pro společnost ABC však tato možnost nepředstavuje potenciál, jelikož nabízí velmi specifický produkt a služby pro poměrně úzký okruh zákazníků.

Zaslání adresné nabídky už vyžaduje znalost minimálně jména a adresy, tedy osobních údajů. V tomto případě společnost potřebuje prokazatelný souhlas se zpracováním osobních údajů dané osoby a pokud tento souhlas nezahrnuje také souhlase se zasíláním marketingových nabídek, bylo by zaslání takové reklamní nabídky, byť v listinné podobě, v rozporu se zákonem.

Z výše zmíněného vyplývá, že společnost ABC jedná v mnoha případech v rozporu se zákonem. Zasíláním nevyžádaných obchodních sdělení porušuje ZIS. Dal-

ším nezákonným jednáním je zpracování osobních údajů bez souhlasu subjektu údajů a také neplnění zákonných povinností správce osobních údajů podle ZoOOÚ.

Za takové jednání hrozí společnosti nemalé sankce. Nedodržením svých zákonných povinností nebo zpracováním osobních údajů bez souhlasu subjektu údajů se společnost může dopouštět správního deliktu podle § 45 ZoOOÚ, za což jí může být ÚOOÚ uložena pokuta až 5 000 000 Kč. Zasíláním nevyžádaného obchodního sdělení nebo obchodního sdělení nesplňujícího všechny zákonné náležitosti může společnost naplnit skutkovou podstatu správního deliktu podle § 11 ZIS, za něž jí ÚOOÚ může uložit pokutu až do výše 10 000 000 Kč.

Doporučení pro společnost ABC

V oblasti ochrany osobních údajů zákazníků se společnost ABC opakovaně dopouští mnoha méně či více závažných pochybení. Proto navrhuji následující:

- Zajistit fyzickou ochranu osobních údajů – fyzické dokumenty uchovávat v uzamykatelné skříňce, dokumenty v elektronické podobě zabezpečit heslovaným přístupem.
- Určit okruh oprávněných osob a ty řádně o jejich povinnostech proškolit.
- Zpracovávat pouze osobní údaje, k jejichž zpracování dané osoby udělily společnosti ABC informovaný souhlas.
- Osobní údaje zpracovávat pouze v souladu s definovaným účelem, a to pouze v rozsahu nezbytném pro splnění tohoto účelu.
- Neslučovat osobní údaje získané pro různé účely.
- Zpracovávat pouze přesné osobní údaje a pokud je to potřeba, tyto údaje aktualizovat.
- Upravit webový formulář – jasně definovat souhlas se zpracováním osobních údajů a přidat možnost vyslovit souhlas se zasíláním obchodního sdělení.
- Elektronické obchodní sdělení zasílat pouze na základě předem uděleného souhlasu. Neztotožňovat souhlas se zpracováním osobních údajů se souhlasem se zasíláním obchodních sdělení.
- Elektronická obchodní sdělení jasně označit.
- Doporučuji nepokračovat ve vyhledávání kontaktů na internetu a následném zasílání obchodních sdělení, jelikož zde společnost nezískala souhlas daných osob.
- Adresná reklamní sdělení poštou zasílat pouze s předchozím souhlasem. Bez souhlasu lze poštou zasílat pouze neadresná sdělení.

4.4.3 Ochrana osobních údajů podle GDPR

Výše byla provedena analýza ochrany osobních údajů ve společnosti ABC podle nynější právní úpravy. Od 25.5.2018 však vstoupí v platnost Obecné nařízení o ochraně osobních údajů neboli GDPR, které přináší nové přísnější povinnosti správců i zpracovatelů osobních údajů a také mnohem vyšší sankce za jejich nedodržování.

I když toto nařízení vstoupí v platnost až za rok, na změny vyplývající z této normy by se měla společnost připravovat již nyní. Bude potřeba upravit či změnit

obchodní a marketingové procesy, smluvní ujednání, bezpečnostní opatření i ICT infrastrukturu. Uvedení společnosti do souladu s GDPR bude dlouhodobým procesem, který s sebou přinese i nemalou časovou a finanční zátěž.

Z nového nařízení bude plynout mnoho nových povinností, např. datový a bezpečnostní audit a jmenování pověřence pro ochranu osobních údajů.

Jelikož se jedná o velice rozsáhlou a složitou problematiku, doporučuji společnosti ABC konzultovat tuto problematiku s odborníkem, a to ještě před započetím implementace organizačních i technických opatření vedoucích k uvedení společnosti do souladu s GDPR. Přípravu pouze vlastními silami bez konzultace se specialistou určitě nedoporučuji.

Ze změn, které GDPR přinese zde zmíním jednu, která se dle mého názoru společnosti ABC dotkne nejvíce, a tou je souhlas se zpracováním osobních údajů. Osobní údaje bude možné zpracovávat rovněž pouze se souhlasem subjektu údajů, přičemž tento souhlas musí nově být učiněn svobodně, musí být konkrétní, informovaný, jednoznačný a ničím nepodmíněný. Pokud tyto náležitosti souhlas nesplňuje, je nutné uvést tuto skutečnost do souladu, a to ještě před účinností nového nařízení. Po 25.5.2018 již bude nutné nevyhovující souhlasy se zpracováním osobních údajů nahradit souhlasy novými.

Zde spatřuji největší problém pro společnost ABC, jelikož ve své databázi eviduje velké množství kontaktů bez souhlasu se zpracováním osobních údajů a velké množství kontaktů, které společnosti souhlas v minulosti sice udělili, ten však už mnohdy nelze dokázat a nesplňuje některé náležitosti podle GDPR.

Přípravu na GDPR rozhodně nedoporučuji podceňovat, jelikož sankce, které za nesplnění povinností hrozí, by pro společnost ABC byly prakticky likvidační. Za porušení např. povinnosti jmenovat pověřence hrozí pokuta až 10 000 000 EUR, za nesplnění jiných povinností dokonce až 20 000 000 EUR nebo 4 % z celkového ročního obratu společnosti (vyšší z obou možností). (Škorničková, 2016)

5 Diskuze

Společnost ABC v rámci své činnosti zpracovává poměrně velké množství nejrůznějších informací. Mnohé z nich představují pro ni nebo pro její klienty či obchodní partnery významnou hodnotu. Ochrana těchto informací zde proto představuje důležitou otázku.

Informace týkající se samotné společnosti ABC podnikatel ochraňuje ve svém vlastním zájmu. Jiné informace firma chrání a utajuje na základě smluvního ujednání, u jiných jí tato povinnosti vyplývá přímo ze zákona.

Ochrana informací je smluvně ošetřena jak ve vztahu k zaměstnancům společnosti, tak ve vztahu ke klientům a obchodním partnerům. Společnost věnuje pozornost také fyzické ochraně informací ve formě zabezpečených přístupů k datům v elektronické podobě apod. Na základě provedené analýzy lze konstatovat, že společnost si je vědoma důležitosti ochrany informací, avšak v mnoha ohledech postupuje nedůsledně, mnohdy dokonce v rozporu se zákonem.

V oblasti ochrany vlastního obchodního tajemství, know-how a důvěrných informací vůči klientům a obchodním partnerům společnosti doporučuji především jasnou definici chráněných informací a povinností v oblasti bezpečnostních opatření. Odstranění chyb a nejasností, které se v současnosti v moha smlouvách nacházejí, pomůže společnosti zajistit efektivní ochranu jejích důležitých informací a v případě sporu s druhou smluvní stranou také lepší vymahatelnost svých práv. Navrhuji také určit výši smluvní pokuty vždy individuálně pro jednotlivý případ, čímž se společnost může vyhnout sporu ohledně nepřiměřenosti smluvní pokuty.

Rizika plynoucí z nevyhovující smluvní úpravy spočívají především ve vyzrazení či zneužití důležitých informací, což může mít za následek oslabení až ztrátu získané konkurenční výhody podnikatele.

Ochranu těchto informací vůči zaměstnancům společnosti navrhuji upravit pomocí jasně definovaných pravidel upravených v pracovní smlouvě, dohodě o mlčenlivosti nebo v pracovním řádu, přičemž za nejvhodnější variantu považuji právě pracovní řád vzhledem k možnosti jeho jednostranné úpravy ze strany zaměstnavatele. Rozhodně doporučuji odstranit současnou roztříštěnost úpravy v několika dokumentech. Z úpravy povinností zaměstnanců v oblasti ochrany informací musí být jasná především závaznost a důležitost této problematiky. Doporučuji nepodcenit především seznámení nových zaměstnanců s jejich povinnostmi, stávající zaměstnance navrhuji pravidelně školit. Zaměstnanci jsou totiž obecně nejslabším článkem v oblasti ochrany informací. Jasně nastavenými pravidly, se kterými budou všichni zaměstnanci důkladně seznámeni, může společnost zabránit úniku cenných informací, jejich zneužití a opět také ztrátě konkurenční výhody.

Společnost je nejen poskytovatelem svých cenných informací, ale také příjemcem a zpracovatelem cenných informací svých zákazníků. Zde se k jejich ochraně smluvně zavázala, z čehož jí plynou mnohé povinnosti a v případě jejich nedodržení také nemalé sankce.

Společnost ABC dodává svou aplikaci často velkým společnostem, čímž se dostává do postavení slabšího smluvního partnera. V těchto případech je jí mnohdy předložen návrh dohody o mlčenlivosti obsahující pro ni nevýhodná ujednání. Doporučuji tyto smlouvy řádně prostudovat a v případě pochybností se poradit s odborníkem. Smlouva by měla upravovat podmínky ochrany informací obou smluvních stran, nikoli pouze té silnější. V případě, že jsou navrženy neúměrně vysoké sankce v kombinaci s obtížně splnitelnými povinnostmi, je dle mého názoru potřeba zvážit, zda je pro společnost vůbec vhodné danou spolupráci navázat.

Společnosti dále doporučuji důsledně dodržovat všechna bezpečnostní opatření a jiné povinnosti z těchto smluv vyplývající. K dodržení těchto závazků je nutné, aby o nich byli zaměstnanci řádně poučeni. Kdyby došlo k porušení mlčenlivosti nedbalostí zaměstnance, odpovědnost je přesto na straně společnosti ABC.

V případě porušení smluvních povinností či soudního sporu hrozí podnikateli nejen riziko platby často velmi vysoké smluvní pokuty či náhrady škody, ale také ztráta dobrého jména na trhu. Z tohoto pohledu doporučuji nebrat ochranu informací klientů a obchodních partnerů na lehkou váhu.

Další skupinou chráněných informací jsou osobní údaje. Společnost je správcem osobních údajů svých zaměstnanců a svých klientů.

V oblasti ochrany osobních údajů zaměstnanců se společnost v několika ohledech dopouští jednání v rozporu se zákonem o ochraně osobních údajů. Jedná se zejména o zpracování některých osobních údajů nad rámec svých zákonných povinností bez souhlasu zaměstnanců, uchovávání osobních údajů neúspěšných uchazečů o zaměstnání po skončení výběrového řízení a také uchovávání osobních údajů osob po skončení pracovního poměru ve společnosti ABC.

Největší pochybení ze strany společnosti ABC spatřuji v ochraně osobních údajů svých zákazníků a obchodních partnerů. Společnost zpracovává velké množství osobních údajů bez souhlasu k tomuto zpracování a nedodržuje některé své povinnosti vyplývající ze zákona o ochraně osobních údajů, zejména přesnost a aktuálnost zpracovávaných údajů a dále zpracování pouze v souladu s účelem, ke kterému byly údaje shromážděny. Dále neplní svou oznamovací povinnost vůči Úřadu pro ochranu osobních údajů, která vyplývá z § 16 tohoto zákona. Tím by společnost mohla naplnit znaky správního deliktu podle § 45 odst. 1. zákona o ochraně osobních údajů, za což jí hrozí pokuta ve výši až 5 000 000 Kč. V případě, že tímto dojde k ohrožení většího počtu osob, může se pokuta vyšplhat až na 10 000 000 Kč.

Společnost propaguje své produkty i prostřednictvím zasílání elektronických obchodních sdělení. Za nevyžádané obchodní sdělení, tedy zaslání sdělení bez souhlasu adresáta nebo za obchodní sdělení neobsahující všechny náležitosti hrozí společnosti pokuta ve výši až 10 000 000 Kč za správní delikt podle § 11 zákona č. 480/2004 Sb., o některých službách informační společnosti.

Začátkem roku 2017 podal jeden ze zákazníků společnosti ABC stížnost u Úřadu pro ochranu osobních údajů týkající se nevyžádaného obchodního sdělení, které od společnosti obdržel. Úřad zaslal společnosti ABC výzvu k nápravě chybného stavu, tedy vymazání daného kontaktu z databáze společnosti.

Kontakt na tuto osobu byl pravděpodobně získán pomocí vlastního vyhledání na internetu, k oslovení tedy došlo bez jejího souhlasu. Společnost ABC tento kontakt ze své databáze vymazala, avšak velké množství kontaktů bez souhlasu pro zpracování osobních údajů ve své databázi dále eviduje a je velmi pravděpodobné, že je v budoucnu osloví některou ze svých kampaní, i když nemá souhlas k zasílání obchodních sdělení. Společnost ABC si je vědoma důsledků, které toto počínání může mít, avšak věří, že tato stížnost byla pouze ojedinělým případem. Navíc stížnost nepřinášela žádné závažnější důsledky, které by vedení společnosti ABC přiměly v tomto jednání dále nepokračovat.

Společnost přijala mnoho z návrhů uvedených v této diplomové práci, např. se registrovala u Úřadu pro ochranu osobních údajů jako správce osobních údajů svých zákazníků, upravila webový formulář, plánuje revizi databáze svých potenciálních zákazníků, změnila znění dohody o mlčenlivosti uzavírané s novými zaměstnanci aj. Mnohé však měnit nehodlá, zde jde zejména o vyhledání a oslovení potenciálních zákazníků na internetu či oslovování kontaktů získaných z doporučení. Vedení společnosti je přesvědčeno, že pokud se tak neděje hromadně, o protiprávní jednání se nejedná. Domnívá se, že některé skupiny zákazníků totiž jiným než tímto „tradičním“ způsobem oslovit nelze.

Dle mého názoru se však jedná o poměrně nezodpovědný přístup. Rozesíláním nevyžádaných obchodních sdělení a shromažďováním osobních údajů bez souhlasu daných subjektů údajů společnost riskuje nejen vysokou pokutu od Úřadu pro ochranu osobních údajů, ale také dobré jméno společnosti. Úřad pro ochranu osobních údajů eviduje všechny stížnosti podané na podnikatele a může u něj provést kontrolu. Výsledky těchto kontrol jsou veřejně přístupné na webových stránkách tohoto úřadu.

Doporučení, která navrhuji, mohou tato rizika značně omezit. Zavedení těchto doporučení by společnosti ABC nepřineslo významné náklady, jednalo by se zejména o organizační a provozní změny. Cena za konzultaci smluv s právním poradcem dle mého názoru představuje pouze zanedbatelný zlomek ceny rizik, kterým se společnost v případě nezavedení mých doporučení vystavuje.

Mnoho změn do fungování společnosti jistě přinese také nové Obecné nařízení o ochraně osobních údajů (GDPR), které přináší mnohem přísnější pravidla a vyšší sankce.

Společnost ABC je mladou firmou s firemní kulturou založenou na důvěře. Důvěra ve své zaměstnance se však musí opírat o jasná pravidla a informovanost. Ve vztazích s obchodními partnery není prostor pro naivitu. Ta je dle mého názoru neslučitelná s profesionalitou společnosti, zvláště v oblasti IT, kde informace jsou to nejcennější, co firma má.

6 Závěr

Tématem této diplomové práce byla ochrana informací v obchodní společnosti zabývající se IT.

Cílem práce bylo na základě analýzy současného stavu ochrany informací definovat nedostatky a navrhnout vhodná řešení respektující současnou právní úpravu České republiky.

Nejdříve byla provedena analýza smluv uzavíraných se zaměstnanci, zákazníky a obchodními partnery zajišťujících ve společnosti ochranu obchodního tajemství, know-how, důvěrných informací a osobních údajů. Hodnocena byla jak ochrana informací týkajících se této společnosti, tak informací týkajících se klientů a obchodních partnerů.

Na základě mnoha zjištěných pochybení byla formulována doporučení pro eliminaci možných rizik a zajištění efektivní ochrany informací. Jedním z těchto návrhů je pracovní řád upravující způsob ochrany informací v této firmě.

Posledním krokem bylo zhodnocení ekonomických dopadů plynoucích z možných sankcí a nedostatků současného stavu ochrany informací, ale také ze zavedení navržených doporučení.

7 Literatura

Knižní zdroje:

ACHOUR, GABRIEL A MARTIN PELIKÁN. *Náhrada škody a nemajetkové újmy v občanskoprávních a obchodních vztazích*. Ostrava: Key Publishing, 2015. Právo (Key Publishing). ISBN 978-80-7418-231-0.

BARTÍK, VÁCLAV A EVA JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: vybrané otázky. 2. vyd*. Praha: Linde, 2010. Praktická právnická příručka. ISBN 978-80-7201-813-0.

BĚLINA, MIROSLAV. *Pracovní právo. 6., dopl. a podstatně přeprac. vyd*. V Praze: C.H. Beck, 2014. Academia iuris (C.H. Beck). ISBN 978-80-7400-283-0.

ČADA, KAREL. *Chránit / nechránit, to je otázka: výsledky výzkumu a vývoje, jejich ochrana a komercializace*. Plzeň: Alevia, 2014. ISBN 978-80-905538-0-4.

ČADA, KAREL. *Know-how a obchodní tajemství. Vyd. 1. [i.e. 2. vyd.].* Praha: Úřad průmyslového vlastnictví, 2010. ISBN 978-80-7282-087-0.

ČERNÁ, STANISLAVA, Ivana ŠTENGLOVÁ, Irena PELIKÁNOVÁ a Jan DĚDIČ. *Obchodní právo: podnikatel, podnikání, závazky s účastí podnikatele.* Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-333-4.

GALVAS, MILAN. *Pracovní právo. 2., doplněné a přepracované vydání*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8021-8.

JANSA, LUKÁŠ A PETR OTEVŘEL. *Softwarové právo. 2. vyd.* Brno: Computer Press, 2014. ISBN 978-80-251-4201-1.

MAISNER, MARTIN. *Základy softwarového práva*. Praha: Wolters Kluwer Česká republika, 2011. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7357-638-7.

MAŠTALKA, JIŘÍ. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008. Beckova edice ABC. ISBN 978-80-7400-033-1.

MATOUŠOVÁ, MIROSLAVA A LADISLAV HEJLÍK. *Osobní údaje a jejich ochrana. 2., dopl. a aktualiz. vyd.* Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 978-80-7357-322-5.

NOVÁK, DANIEL. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5.

Ochrana osobních údajů: vybrané otázky: příručka pro podnikatele. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011. ISBN 978-80-210-5572-8.

Ochrana osobních údajů na pracovišti: [příručka pro zaměstnance]. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2014. ISBN 978-80-210-6819-3.

POLČÁK, RADIM. *Právo na internetu: spam a odpovědnost ISP*. Brno: Computer Press, 2007. Právo a IT. ISBN 978-80-251-1777-4.

RODRYČOVÁ, DANUŠE A PAVEL STAŠA. *Bezpečnost informací jako podmínka prosperity firmy.* Praha: Grada, 2000. Manažer. ISBN 80-7169-144-5.

ŠILEROVÁ, EDITA, KLÁRA HENNYEYOVÁ A N. N. BALAŠOVA. *Informační systémy v podnikové praxi.* Praha: Powerprint, 2016. ISBN 978-80-87994-78-8.

ŠIMEČKOVÁ, EVA. *Konkurenční jednání zaměstnance.* Praha: Linde, 2008. ISBN 978-80-7201-738-6. Dostupné také z: http://kramerius.mzk.cz/search/handle/uuid:7453ea70-5b86-11e5-bf4b-005056827e51

ŠTENGLOVÁ, IVANA. *Obchodní tajemství: praktická příručka.* Praha: Linde, 2005. ISBN 80-7201-559-1.

TINTĚRA, TOMÁŠ. *Smluvní pokuta v ČR a Evropě*. Praha: Leges, 2015. Teoretik. ISBN 978-80-7502-095-6.

WEBSTER, FRANK. *Theories of the information society*. 3rd ed. London: Routledge, 2006. ISBN 9780415406321.

Internetové zdroje:

CALLAGHAN, IDA. *Předsmluvní odpovědnost*. In: Epravo.cz [online]. Praha, 2015 [cit. 2017-03-05]. Dostupné z: https://www.epravo.cz/top/clanky/predsmluvni-odpovednost-96340.html

Často kladené otázky k zákonu č. 480/2004 Sb.: Nevyžádaná obchodní sdělení: Úřad pro ochranu osobních údajů [online]. Praha, 2013 [cit. 2017-02-22]. Dostupné z: https://www.uoou.cz/casto-kladene-otazky-k-zakonu-c-480-2004-sb/ds-1507/archiv=0&p1=1493#b3

Často kladené otázky k zákonu č. 480/2004 Sb., o některých službách informační společnosti. In: Epravo [online]. 2004 [cit. 2017-03-26]. Dostupné z: https://www.epravo.cz/top/clanky/casto-kladene-otazky-k-zakonu-c-4802004-sb-o-nekterych-sluzbach-informacni-spolecnosti-28646.html?mail

DOLEČEK, MAREK. *Obchodní tajemství*. In: Bussinessinfo.cz [online]. Praha, 2015 [cit. 2017-03-06]. Dostupné z: http://www.businessinfo.cz/cs/clanky/obchodni-tajemstvi-ppbi-50787.html#!&chapter=2

GDPR.cz: Obecné nařízení o ochraně osobních údajů prakticky [online]. Praha, 2015 [cit. 2017-03-28]. Dostupné z: www.gdpr.cz

HAVLÍK, MARTIN. *Pojetí smluvní pokuty v NOZ s akcentem na (ne)moderaci smluvní pokuty.* In: Epravo.cz [online]. Praha, 2013 [cit. 2017-04-24]. Dostupné z: https://www.epravo.cz/top/clanky/pojeti-smluvni-pokuty-v-noz-s-akcentem-na-nemoderaci-smluvni-pokuty-92058.html

HINDER, DAVID A KEMSLEY BRENNAN. *Information security: risks, examples and ways forward. Governance Directions* [online]. 2014, **66**(8), 484-488 [cit. 2017-03-26]. ISSN 22034749. Dostupné z:

http://search.ebscohost.com/login.aspx?direct=true&db=bth&an=101914988&scope=site

JANEČKOVÁ, EVA A VÁCLAV BARTÍK. *Fotografie v osobním spisu zaměstnance z hlediska zákona o ochraně osobních údajů*. In: Daňaři online [online]. 2012 [cit. 2017-03-15]. Dostupné z: http://www.danarionline.cz/archiv/dokument/doc-d39537v49559-fotografie-v-osobnim-spisu-zamestnance-z-hlediska-zakona-o-ochrane/

KARLÍČEK, MIROSLAV A PETR KRÁL. *Marketingová komunikace: jak komunikovat na našem trhu*. Praha: Grada, 2011. ISBN 978-80-247-3541-2.

LOVĚTÍNSKÝ, VOJTĚCH. *Lze smluvně vyloučit právo soudu snížit nepřiměřeně vysokou smluvní pokutu?* In: Epravo.cz [online]. Praha, 2017 [cit. 2017-04-30]. Dostupné z: https://www.epravo.cz/top/clanky/lze-smluvne-vyloucit-pravo-soudu-snizit-neprimerene-vysokou-smluvni-pokutu-105192.html?mail

MAREŠ, DAVID. *Internetová reklama a nevyžádaná obchodní sdělení šířená elektronickými prostředky*. In: Epravo.cz [online]. Brno, 2010 [cit. 2017-04-07]. Dostupné z: https://www.epravo.cz/top/clanky/internerova-reklama-a-nevyzadana-obchodni-sdeleni-sirena-elektronickymi-prostredky-63234.html

SAEED, OMAR HASSAN MOHAMED. *The importance of data protection process in the small and medium enterprises*. International Journal of Research and Reviews in Applied Sciences [online]. 2011, 6(2) [cit. 2017-03-07]. ISSN 2076734X. Dostupné z: http://search.ebscohost.com/login.aspx?direct=true&db=edsoaf&an=edsoaf.a67f8e1d4d018b76eac9186589eefd6890822dd5&scope=site

PAVLÁT, DAVID. *Nevyžádaná obchodní sdělení*. In: Úřad pro ochranu osobních údajů [online]. 2013 [cit. 2017-04-01]. Dostupné z: https://www.uoou.cz/nevyzadana-obchodni-sdeleni/d-6134

Protection of personal data. European Commission [online]. 2017 [cit. 2017-03-15]. Dostupné z: http://ec.europa.eu/justice/data-protection/index_en.htm

RADIČOVÁ, ZUZANA A DAVID BURIAN. *Nová regulace ochrany osobních údajů aneb na jaké změny se připravit.* In: E-pravo.cz [online]. Praha, 2016 [cit. 2017-03-28]. Dostupné z: https://www.epravo.cz/top/clanky/nova-regulace-ochrany-osobnich-udaju-aneb-na-jake-zmeny-se-pripravit-103479.html

ŠKUBAL, JAROSLAV A DANIEL VEJSADA. *Doba uchování pracovněprávních dokumentů.* In: Epravo.cz [online]. Praha, 2013 [cit. 2017-04-01]. Dostupné z: https://www.epravo.cz/top/clanky/doba-uchovani-pracovnepravnich-dokumentu-88494.html

URBAN, BOHDAN. *Zákon o některých službách informační společnosti - co přináší telemarketingovým společnostem a v oblasti spotřebitelských smluv.* In: Epravo [online]. 2004 [cit. 2017-03-26]. Dostupné z: https://www.epravo.cz/top/clanky/zakon-o-nekterych-sluzbach-informacni-spolecnosti-co-prinasi-telemarketingovym-spolecnostem-a-v-oblasti-spotrebitelskych-smluv-28373.html

VALÍČKOVÁ, IRENA. *Jiná výdělečná činnost zaměstnance… kdy jde skutečně o konkurenční doložku*. In: Epravo.cz [online]. Praha, 2016 [cit. 2017-03-11]. Dostupné z: https://www.epravo.cz/top/clanky/jina-vydelecna-cinnost-zamestnance-kdy-jde-skutecne-o-konkurencni-dolozku-101593.html

Zaměstnavatel nesmí ukládat povinnosti nad rámec zákona. In: Veřejný ochránce práv [online]. 2016 [cit. 2017-03-07]. Dostupné z: https://www.ochrance.cz/aktualne/tiskove-zpravy-2016/zamestnavatel-nesmi-ukladat-povinnosti-nad-ramec-zakona/

Právní předpisy:

Nařízení Komise (EU) č. 330/2010
Zákon č. 40/1995 Sb., o provozování rozhlasového a televizního vysílání
Zákon č. 328/1999 Sb., o občanských průkazech a
Zákon č. 329/1999 Sb., o cestovních dokladech
Zákon č. 101/2000 Sb., o ochraně osobních údajů
Zákon č. 121/2000 Sb., autorský zákon
Zákon č. 435/2004 Sb., o zaměstnanosti
Zákon č. 480/2004 Sb., o některých službách informační společnosti
Zákon č. 262/2006 Sb., zákoník práce
Zákon č. 40/2009 Sb., trestní zákoník
Zákon č. 89/2012 Sb., občanský zákoník

Přílohy

A Návrh pracovního řádu společnosti ABC

PRACOVNÍ ŘÁD SPOLEČNOSTI ABC

V souladu s ustanovením § 306 zákoníku práce vydává společnost ABC tuto vnitropodnikovou směrnici Pracovní řád.

Cílem směrnice je upřesnit práva a povinnosti zaměstnanců i zaměstnavatele.

Pracovní řád je závazný jak pro společnost ABC, tak pro všechny její zaměstnance.

S Pracovním řádem jsou zaměstnanci seznámeni v den nástupu do zaměstnání. Povinnost dodržovat Pracovní řád společnosti ABC zaměstnanci potvrzují svým podpisem na pracovní smlouvě.

Pracovní řád je k dispozici všem zaměstnancům ve fyzické podobě v každé z poboček společnosti ABC, a dále v elektronické podobě v interním systému společnosti na adrese …….. .

Kontaktní osobou v případě jakýchkoliv nejasností je ……., případně teamleader příslušného týmu.

Teamleader týmu A je ……..
Teamleader týmu B je ……..
Teamleader týmu C je ……..

1. Povinnosti zaměstnanců v oblasti ochrany informací

Zaměstnanci jsou povinni dodržovat mlčenlivost:

- o všech informacích, které by mohly poškodit dobré jméno zaměstnavatele nebo mu způsobit materiální či jinou újmu;
- o všech důvěrných informacích, obchodním tajemství a o osobních údajích, se kterými se v rámci prací konaných u zaměstnavatele zaměstnanec seznámí, ať už se tyto informace týkají zaměstnavatele nebo jeho obchodních partnerů a zákazníků;
- o skutečnostech týkajících se bezpečnostních opatření chráněných informací.

Obchodní tajemství tvoří podle § 504 občanského zákoníku konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení.

Ve společnosti ABC se jedná zejména o zdrojové kódy, návrhy řešení, různé metodiky výpočtů a analýz, projektové dokumentace, strategické a marketingové plány, cenové kalkulace či databáze zákazníků.

Pod pojmem důvěrné informace se rozumí:

- jakékoliv informace, které zaměstnavatel výslovně označí jako „důvěrné informace“, přičemž se nejedná o nevyhnutelnou podmínku;
- neveřejné údaje o zákaznících zaměstnavatele, informace v obchodních nabídkách včetně ceny, projektové plány, analýzy, obsah obchodních smluv, historie e-mailové komunikace a zápisy z jednání s klienty, jakožto i jiné informace obchodní, výrobní či technické povahy, které se týkají zákazníků a obchodních partnerů zaměstnavatele;
- neveřejné informace o finanční a majetkové situaci zaměstnavatele, informace o marketingové a obchodní strategii, o projektech, plánech a záměrech zaměstnavatele, o jeho obchodních partnerech, klientech, obchodních a jiných kontaktech;
- informace o pracovních a výrobních postupech a metodách a jiném know-how zaměstnavatele;
- zdrojové kódy počítačových programů, bezpečnostní kódy a hesla;
- informace o mzdových podmínkách a jiných formách pracovního ohodnocení,

a to bez ohledu na to, zda byly tyto informace zachyceny v písemné, ústní vizuální nebo elektronické podobě.“

Osobním údajem se podle § 4 ZoOOÚ rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Ve společnosti ABC se jedná zejména o jméno a příjmení, datum a místo narození, věk, korespondenční adresu i adresu trvalého bydliště, rodné číslo, číslo občanského či jiného osobního dokladu, e-mailovou adresu a v případě zaměstnanců i o informace o mzdovém a jiném ohodnocení jednotlivých zaměstnanců a ostatní informace uvedené v osobním dotazníku a osobním spisu zaměstnanců.

Zaměstnanci jsou dále povinni dodržovat veškerá bezpečnostní opatření nařízena zaměstnavatelem.

Není-li si zaměstnanec jistý správným postupem, je povinen poradit se s teamleadrem příslušného týmu.

Porušení mlčenlivosti zaměstnance je závažným porušením jeho povinností, což opravňuje zaměstnavatele k okamžitému zrušení pracovního poměru podle § 55 ZP. Tím není dotčeno právo na náhradu škody ani ušlého zisku.

Závazek mlčenlivosti zaměstnance platí po dobu existence chráněných informací, pokud tohoto závazku nebude zaměstnanec zaměstnavatelem dříve písemně zproštěn. Povinnost zachovávat mlčenlivost o chráněných informacích trvá i po skončení pracovního poměru.