Mendelova univerzita v Brně
Provozně ekonomická fakulta

Ochrana soukromí a osobních údajů zaměstnanců v obchodní společnosti

Diplomová práce

Vedoucí práce:
JUDr. Hana Kelblová, Ph.D.

Bc. Jan Hercík

Brno 2017

Poděkování

Rád bych touto cestou poděkoval JUDr. Haně Kelblové, Ph.D. za vedení mé diplomové práce a za cenné rady, které mi během konzultací poskytla. Dále bych rád poděkoval zaměstnancům firmy XYZ a.s. za jejich vstřícný přístup při komunikaci a za poskytnutí veškerých dat nutných pro tuto práci.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Ochrana soukromí a osobních údajů zaměstnanců v obchodní společnosti** vypracoval/a 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 vědom/a, 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 15. května 2017 _____

Abstract

Hercík, J. Protection of Privacy and Personal data of Employees in a Business Organization. Master's thesis. Brno: Mendel University in Brno, 2017.
The thesis is focused on the protection of personal data and privacy under an employment relationship. The main aim of this thesis is to suggest specific corrective measures to a business organization in order to ensure an alignment between its current situation and the legislation of the Czech Republic. The literary research represents an introduction to the topic of personal data protection and privacy. Definitions of its basic concepts are put into context of the legislation of the Czech Republic. The original research part contains an analysis of personal data protection and privacy measures in a chosen business organization throughout its complete process from staff selection to termination of employment. As a result of a comparison between this analysis and the current legislation of the Czech Republic, proposals to introduce specific corrective measures are presented.

Keywords

personal data, privacy, monitoring of employees, personal data administrator, data subject, The Office for Personal Data Protection

Abstrakt

Hercík, J. Ochrana soukromí a osobních údajů zaměstnanců v obchodní společnosti. Diplomová práce. Brno: Mendelova univerzita v Brně, 2017.
Diplomová práce je zaměřena na ochranu osobních údajů a soukromí v rámci pracovněprávních vztahů. Hlavním cílem práce je navrhnout obchodnímu závodu konkrétní opravná opatření k zajištění souladu jejich situace se současnou právní úpravou v České republice. Obsahem literární rešerše je uvedení do problematiky ochrany osobních údajů a soukromí. Jsou zde definovány základní pojmy uvedené do souvislostí s právní úpravou České republiky. Vlastní práce je věnovaná analýze stavu ochrany osobních údajů a soukromí ve vybraném obchodním závodě v rámci celého procesu od počátku výběrového řízení do ukončení pracovního poměru. Jako výsledek komparace analýzy se současným stavem právní legislativy České republiky jsou uvedeny návrhy na zavedení konkrétních opravných opatření.

Klíčová slova

osobní údaje, soukromí, monitorování zaměstnanců, správce osobních údajů, subjekt údajů, Úřad pro ochranu osobních údajů

Obsah

Seznam použitých zkratek

EÚLP	Evropská úmluva o ochraně lidských práv a základních svobod
GDPR	Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
LZPS	Listina základních práv a svobod
OZ	Zákon č. 89/2012 Sb., občanský zákoník
Pověřenec	Pověřenec pro ochranu osobních údajů (anglicky Data Protection Officer, či DPO)
Směrnice 95/46/ES	Směrnice Evropského parlamentu a Rady č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
Trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
Úmluva č. 108	Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (ETS č. 108, Štrasburk, 28. ledna 1981)
Úřad, ÚOOÚ	Úřad na ochranu osobních údajů
VDLP	Všeobecná deklarace lidských práv
ZoOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů
ZPr	Zákon č. 262/2006 Sb., zákoník práce

1 Úvod

Osobní údaje jsou spojeny s člověkem po celou délku jeho života. Ve chvíli kdy se narodí, je mu přiděleno jméno, příjmení, jedinečné rodné číslo a místo narození. K těmto údajům se postupem času přidávají další, jako jsou místo bydliště, vzdělání, rodinný a zdravotní stav, zaměstnání, dovednosti, schopnosti a spousta dalších. Veškerá tato data pak vytváří celkovou osobnost jedince s důležitými životními milníky a poskytují tak skoro dokonalý odraz daného člověka. Vzhledem k enormnímu počtu těchto informací o jednotlivých osobách, vznikla spousta institucí a subjektů, které tyto informace shromažďují a často i dále zpracovávají. Z toho důvodu je nezbytné, aby tato oblast byla usměrněna zákony a směrnicemi.

Kořeny konceptu ochrany osobních údajů spadají do 70. let minulého století, tuto oblast práva lze tedy považovat za poměrně nový společenský a sociální problém. Mezi zlomové dokumenty při výkladu tohoto práva lze zařadit Úmluvu č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat přijatou Radou Evropy a také Směrnici 95/46/ES, o ochraně fyzických osob, zpracování osobních údajů a jejich volným pohybem. Tato směrnice přikazovala všem členským státům EU chránit soukromí fyzických osob při zpracování jejich dat a také zabezpečit ochranu veškerých základních práv a svobod.

V České republice je problematika s ochranou soukromí pokryta Ústavou, Listinou základních práv a svobod, které tvoří základní stavební kameny pro tvorbu dalších zákonů. Ochranou soukromí a osobních údajů se zabývá také zákoník práce, nový občanský zákoník a zákon č. 101/2000 Sb., o ochraně osobních údajů. Navzdory systému právní úpravy zabývajícího se ochranou osobních údajů neustále dochází k porušování tohoto práva v běžném životě.

Navázání nového pracovního poměru téměř vždy vyžaduje poskytnutí osobních informací, které jsou nezbytné k uzavření plnohodnotné pracovní smlouvy.

Častým fenoménem je, že potencionální zaměstnavatel hledá informace o kandidátovi ještě před osobním setkáním, a to prostřednictvím internetu, nejčastěji sociálních profilů jako je Facebook, Twitter, Google+ a LinkedIn. Už jen z tohoto důvodu je vhodné být opatrný při sdílení obsahu na profilech těchto sociálních sítí, jelikož jakýkoli neadekvátní obsah ve formě nevhodných fotografií či vulgárního statusu by mohl rapidně ohrozit výsledek přijímacího procesu.

V případě že uchazeč byl v rámci přijímacího řízení úspěšný a stal se zaměstnancem tak kromě sdělení svých osobních informací začne být často i monitorován. Pod dohledem je obvykle příchod a odchod do budovy, kde je práce vykonávána a pracovní cesty uskutečněné firemním vozidlem. Tyto a mnohé další formy kontrol a monitoringu slouží k ochraně zaměstnavatele, především k ochraně jeho zájmů a majetku, na druhé straně však zasahují do soukromí zaměstnanců. Je tedy důležité, aby užití kontrol a monitorovacích zařízení bylo přiměřené a nepřekračovalo zákonné hranice.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je na základě podrobné analýzy úrovně ochrany soukromí a osobních údajů v konkrétním obchodním závodu vyhodnotit, jak jsou právní předpisy na ochranu soukromí a osobních údajů zaměstnanců dodržovány a navrhnout konkrétní opravná opatření k zajištění souladu se současnou právní úpravou v České republice.

Součástí návrhů bude vymezení důsledků porušování povinností při zpracování osobních údajů a ochrany soukromí, případných sankcí a také vyčíslení ekonomické náročnosti zavedení konkrétních doporučení v obchodním závodu.

2.2 Metodika

Diplomová práce bude rozdělena na několik částí. První částí bude literární rešerše, ve které budou vymezeny základní pojmy týkající se ochrany osobních údajů, historie vývoje právních pramenů týkající se dané problematiky, představeny orgány zastřešující ochranu osobních údajů v České republice včetně jejich činností. Literární rešerše bude dále také obsahovat informace o tom, jak by měly být osobní údaje ochraňovány a budou vysvětleny možné sankce při porušení zásad zpracování osobních údajů.

Část literární rešerše zaobírající se soukromím pak bude věnována vysvětlení pojmu soukromí a také především monitorování zaměstnanců na pracovišti. Informace v literární rešerši budou podepřeny současnou legislativou České republiky.

V rámci vlastní práce bude nejdříve představen analyzovaný obchodní závod, a to v anonymizované formě, neboť si společnost z důvodů citlivé problematiky nepřála zveřejnit svoje jméno. Tato společnost tedy bude představována a v celé práci referována pod názvem XYZ a.s.

Samotná analýza se bude věnovat úkonům v pracovněprávním postupu společnosti XYZ a.s., který začíná inzerováním volné pracovní pozice, pokračuje výběrovým řízením a vznikem, průběhem a ukončením pracovního poměru. V každé jedné části bude identifikováno a analyzováno, které osobní údaje se dané části týkají, které jsou shromažďovány a jak se s těmito osobními údaji v dané části pracovněprávního postupu zachází. Součástí analýzy průběhu pracovního poměru pak bude rozebírána také problematika ochrany soukromí na pracovišti. Data pro zmíněnou analýzu budou čerpána z různých vnitropodnikových směrnic, řádů a z rozhovorů s odpovědnými osobami za dané problematiky ze společnosti XYZ a.s.

Veškeré zjištěné výsledky analýzy budou komparovány s platnou právní úpravou České republiky a výsledky této komparace budou základem pro jednotlivé návrhy na zajištění souladu současného stavu s platnou právní úpravou České republiky.

Každý návrh bude obsahovat uvedení do problému, navrhovanou nápravu, vyčíslení potenciálních sankcí, pokud to bude možné a bude zakončen kalkulací nákladů na zavedení daného návrhu. Tyto návrhy budou určené právnímu oddělení společnosti XYZ a.s., které na jejich základě může zajistit nápravu.

3 Literární rešerše

3.1 Legislativa ochrany osobních údajů

3.1.1 Mezinárodní prameny práva

Zvyšující se pohyb lidí mezi státy, rostoucí mezinárodní spolupráce a globalizace celkově začala vyžadovat nové požadavky na poli mezinárodní koordinace v rámci ochrany osobních dat. Z toho důvodu Organizace pro ekonomickou spolupráci a rozvoj (OECD) vydala 23. září 1980 Průvodce o ochraně soukromí a o přenosu osobních dat přes hranice států. V tomto dokumentu byly poprvé definovány pojmy jako správce, subjekt údajů, osobní údaje, přenos přes hranice a další, které jsou od té doby používány ve všech dalších dokumentech. (Janečková a Bartík, 2016)

Ochrana osobních údajů patří mezi základní lidská práva a díky tomu je garantována řadou národních i mezinárodních právních předpisů. Mezi jeden z prvních komplexních mezinárodních právních předpisů může být zařazena Úmluva č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat, přijatá 28. ledna 1981 Radou Evropy. Ta zajišťovala fyzickým osobám ve smluvních zemích úctu k jejich právům a základním svobodám vztahujícím se k automatizovanému zpracování osobních údajů. (ÚOOÚ, 2011)

Úmluva č. 108 vydržela v nezměněné podobě po dobu dvaceti let, v roce 2001 byla rozšířena Dodatkovým protokolem o orgánech dozoru a toku údajů přes hranice a v této podobě je zatím i dnes. Česká republika ratifikovala Úmluvu č. 108 včetně Dodatkového protokolu dne 24. září 2013. (Janečková a Bartík, 2016)

24. října 1995 pak byla v rámci Evropské unie přijata směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, která má obecnou povahu, vychází z Úmluvy a výrazně ji rozšiřuje a prohlubuje. Kromě ní upravují ochranu osobních údajů ještě další směrnice, které na Směrnici 95/46/ES navazují a doplňují ji. Cílem Směrnice 95/46/ES je usnadnit volný pohyb osobních údajů v rámci členských států Evropské unie a zároveň zaručit jejich nejvyšší možnou míru ochrany. (ÚOOÚ, 2011)

Janečková a Bartík (2016) dodávají, že Směrnice 95/46/ES *„stanovuje požadavky na technickou bezpečnost zpracování dat, ukládá povinnost oznamovat zpracování osobních údajů a mít souhlas dotčené osoby se zpracováním, požaduje vytvoření nezávislého orgánu dozoru, rozšiřuje ochranu osobních údajů také na neautomatizovaně zpracovávané údaje a údaje přenášené mimo Evropskou unii a definuje zvláštní kategorii údajů, tzv. citlivé údaje“*.

Směrnice 95/46/ES byla do české legislativy implementována v rámci zákona č. 101/2000 Sb., o ochraně osobních údajů. (Neuwirt, 2003)

3.1.2 Česká legislativa

Těsně před rozpadem Československé republiky byl vydán zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl vydán k provedení Úmluvy 108. Jeho hlavním nedostatkem byl fakt, že částečně i z důvodu Československé republiky blížící se k rozpadu, nevznikl žádný nezávislý dozorový orgán, který by dodržování zmíněného zákonu hlídal. Zákon také postrádal jakákoliv sankční ustanovení. Z těchto důvodů nebyl zákon v praxi příliš respektován. (Maštalka, 2008)

V rámci České republiky již byl problém absence nezávislého dozorového orgánu vyřešen zákonem č. 101/2000 Sb. o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů, který se vztahuje k článkům 10 a 17 (právo na informace a na ochranu soukromí) Listiny základních práv a svobod a tento zákon se stal v naší republice hlavním zákonem upravujícím ochranu osobních údajů. Dále se ochraně osobnosti, která s ochranou osobních údajů souvisí, věnuje nový občanský zákoník (zákon č. 89/2012 Sb., dále jen OZ) účinný od 1. ledna 2014. V České republice se o ochranu osobních údajů stará jediný orgán, a to Úřad pro ochranu osobních údajů. (ÚOOÚ, 2011)

Maštalka (2008) dodává, že z citovaných článků 10 a 17 vyplývá, že ochrana soukromí a osobních údajů není neomezená. Zdůvodňuje to tím, že zmíněné ochrany jsou garantovány proti neoprávněným zásahům, tím pádem musí existovat i zásahy oprávněné.

V rámci ZoOÚ je z jeho působnosti vyjmuto zpracování osobních údajů pro osobní potřebu, což může v praxi znamenat vedení různých adresářů používaných pro osobní styk. I takové údaje mohou do určité míry být bez porušení zákonů předávány mezi osobami, nicméně pouze při zachování rámce ryze osobních potřeb. Zveřejněním, případně komerčním použitím, takového seznamu by se již režim zákona o ochraně osobních údajů uplatňoval se všemi důsledky. (Maštalka, 2008)

ZoOÚ byl od roku 2000, kdy byl přijat, již 23krát novelizován. Některé z těchto novel ale dosud ještě nejsou účinné. (Janečková a Bartík, 2016)

3.1.3 Principy právní úpravy v zákoně o ochraně osobních údajů

Úmluva č. 108 stanovuje devět základních zásad ochrany osobních údajů, které si pak každá země, která úmluvu ratifikovala, musí promítnout do svých zákonů či jiných právních předpisů. (Mates a spol., 2012)

1. **Zásada legitimity zpracování**, která dle ZoOÚ zajišťuje, že osobní údaje budou získávány a také zpracovány legálním způsobem. Z této zásady také vyplývá, že osobní údaje mohou být zpracovány, až na zákonné výjimky, pouze se souhlasem subjektu údajů.
2. **Zásada omezení účelem** stanovuje, že zpracovávané osobní údaje musí mít specifický, vyjádřený a legitimní účel, a také, že údaje nesmí být zpracovávány pro jiný účel, než bylo původně stanoveno. V ZoOÚ se první část této zásady považuje za splněnou, tedy že správce již určil účel shromažďová-

ní osobních údajů a vyjadřuje se k této zásadě v § 5 odst. 1 písm. d): „*Shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu*“

3. **Zásada časového omezení** stanovuje, že shromažďované osobní údaje mohou být uchovávány pouze po dobu nezbytnou pro naplnění stanoveného účelu. Poté mohou být tyto údaje uchovávány pouze pro účely výzkumů. V ZoOÚ je možno tuto zásadu nalézt v § 5 odst. 1 písm. e), která rozvíjí tuto zásadu v tom, že po uplynutí doby nezbytné k naplnění účelu zpracování se musí údaje anonymizovat pro ochranu subjektu údajů.
4. **Zásada potřebnosti a přiměřenosti**, která může být také uvedena jako zásada nezbytnosti, poukazuje na to, že zpracovávány by měly být pouze nezbytné údaje pro dosažení stanoveného účelu. Nezbytnost by měla být na paměti správce po celou dobu shromažďování údajů. Pokud některé osobní údaje, které na počátku zpracovávání byly nezbytné, ztratí v dalších etapách zpracování tuto vlastnost, měly by být vymazány z paměťových nosičů, je-li to technicky možné. V ZoOÚ je možno tuto zásadu nalézt obsaženou v § 5 odst. 1 písm. d) a f).
5. **Zásada průhlednosti** umožňuje subjektu údajů vyžadovat informace o všech okolnostech zpracování osobních údajů, které se k jeho osobě vztahují, v úplné a srozumitelné formě. V ZoOÚ je tato zásada promítnuta v § 11 takto: „*Správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy*.“
6. **Zásada bezpečnosti** se zaobírá nutností zajištění vhodných bezpečnostních opatření pro ochranu shromažďovaných osobních údajů. K osobním údajům musí být vyloučen neoprávněný přístup, jejich neoprávněné změny či šíření, ale i neoprávněnému zničení či ztrátě. Do zmíněných bezpečnostních opatření lze zahrnout personální (zda jsou osoby pracující s osobními údaji důvěryhodné), technické (pokud jsou údaje zpracovávány pomocí výpočetní techniky) a organizační oblasti. Povinnost vyhodnotit rizika a zajistit odpovídající opatření má jak správce, tak i zpracovatel osobních údajů a to z důvodu, že správce nemusí provádět všechny kroky zpracování. V ZoOÚ se zásadě bezpečnosti věnuje § 13.

   Maštalka (2008) dodává, že i v případě, kdy správce neprovádí všechny kroky zpracování, je správce za veškeré kroky zodpovědný.

7. **Zásada práva přístupu k datům** znamená, že subjekt údajů má právo informovat se o zpracování svých osobních údajů. Požádá-li o tyto informace, správce je povinen mu je bez zbytečného odkladu poskytnout. Správce má v takovém případě právo požadovat za poskytnutí informací přiměřenou úhradu, která však nesmí převýšit náklady na zpracování a poskytnutí daných informací. V ZoOÚ se této problematice věnuje § 12.

8. **Zásada práva na opravu a výmaz** stanoví, že osobní údaje musí být zpracovávány pouze v pravdivé, přesné a pokud možno aktuální formě. Pokud správce zjistí nesrovnalost v osobních údajích, musí nepřesné či nepravdivé údaje ihned blokovat a neprodleně začít s postupem pro odstranění zmíněných nesrovnalostí. Zákon umožňuje, aby tyto údaje byly po určitou dobu blokovány, pokud se však nepodaří učinit nápravu, musí zmíněné údaje jednou pro vždy zlikvidovat. Určitá doba, po kterou mohou být osobní údaje blokovány, však v zákoně není číselně uvedena.
9. **Zásada nezávislého dozoru** udává, že stát má povinnost zajistit nejméně jeden nezávislý orgán, který bude dodržovat dozor nad ochranou a zpracováním údajů. V případě, že je dozorových orgánů více, musí být nezávislé i mezi sebou. (Mates a spol., 2012)

3.2 Základní pojmosloví

3.2.1 Osobní údaj

Původní definice pojmu osobní údaj se nachází v Úmluvě 108 ve článku 2, kde je definovaná následujícím způsobem: „*Osobní údaje znamenají každou informaci týkající se identifikované nebo identifikovatelné fyzické osoby*.“ (Úmluva č. 108, 1981)

V rámci ZoOÚ lze nalézt pojem osobní údaj v §4 písm. a) definovaný jako „*jakoukoliv informaci 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*“. (ZoOÚ, 2000)

Jak je možné si všimnout, v rámci ZoOÚ je pojem osobní údaj rozpracován více do hloubky a identifikovaná, respektive identifikovatelná, fyzická osoba je zde vztažena k tomu, zda se dá přímo či nepřímo určit podle vypsaných prvků ve zmíněné definici. Základním principem určitelnosti je jednoznačná odlišitelnost od všech ostatních. Musí tedy danou osobu být schopno z těchto údajů poznat a kontaktovat. Paní v hnědých šatech se žlutým kloboukem lez potkat na ulici pravděpodobně více a není tedy možné jednoznačně určit, ke komu se údaj vztahuje. Jako základní identifikátory se vybízí jméno a příjmení, podle kterého je možné osobu odlišit od ostatních a adresu, na které jé možné danou osobu nalézt, případně lze ještě přidat datum narození, čímž výčet osobních údajů rozhodně nekončí, nicméně pro nástin určitelnosti to prozatím postačí. Z příkladu vyplývá, že souhrn osobních údajů umožňuje odlišení fyzické osoby od ostatních osob, a tedy i její základní určení. (Maštalka, 2008)

3.2.2 Zpracování osobních údajů

Ne každý osobní údaj podléhá ochraně osobních údajů. Patří tam pouze osobní údaje zpracovávané a z toho důvodu je vhodné pojem zpracování osobních úda-

jů objasnit. Jako zpracování je možno považovat jakékoliv prováděné operace či soustavy operací s osobními údaji. Mezi hlavní operace, které by měly zajistit osobní údaje od získání, přes uchování k tomu, aby údaje mohly být jednoduše dostupné a využitelné, dle Maštalky (2008) patří:

- Shromažďování – operace, kterou se získávají osobní údaje, ověření daných údajů, jejich transformace do formy, ve které budou uchovávány a samotné uložení
- Uchovávání – do této operace patří začlenění osobních údajů do určité databáze
- Zpřístupňování – znamená postoupení osobních údajů k jejich využití
- Blokování – za účelem vyloučení určitých údajů z dalších operací, pokud je u daných údajů prověřována přesnost
- Likvidace osobních údajů – anonymizace, či úplné smazání za účelem trvalého vyloučení z dalšího zpracování

Zmíněné operace budou patřit do zpracování údajů podle zákona pouze v případě opakované činnosti. Nahodilé nakládání s osobními údaji režimu zákona o ochraně osobních údajů nepodléhá, viz § 3 odst. 4 ZoOÚ. (Fialová, 2016)

3.2.3 Subjekt údajů

Subjektem údajů se myslí fyzická osoba, ke které se osobní údaje vztahují. Tato osoba musí být určená nebo alespoň určitelná. Matoušková a Hejlík (2008) upozorňují na to, že určení v tomto smyslu neznamená určení totožnosti.

Dle § 23 Občanského zákoníku fyzická osoba vzniká narozením a zaniká smrtí. Z důvodu, že ZoOÚ pojem fyzické osoby dále nedefinuje, vyplývá ze zmiňovaného paragrafu OZ, že se osobní údaje týkají především žijící fyzické osoby. Podle současné české legislativy veškeré osobní údaje, které se k subjektu údajů vážou, přestávají po úmrtí daného subjektu údajů být osobními údaji a ZoOÚ se stává neaplikovatelný. Veškeré zpracované údaje o daném subjektu by tak po jeho úmrtí měly být zlikvidovány. (Maštalka, 2008)

3.2.4 Správce a zpracovatel

Správcem může být jak fyzická tak i právnická osoba, ale platí, že se musí jednat o právní subjekt. Jako správce nemůže být označeno například pouhé personální oddělení firmy. Správce určuje účel a způsob, jakým budou osobní údaje zpracovávány, a za zpracování odpovídá. Součástí správcových povinností je i samotné zpracování osobních údajů. Zároveň je však v § 4 ZoOÚ uvedeno, že správce může zpracováním údajů zmocnit nebo pověřit zpracovatele, nicméně odpovědnosti za zpracování se tímto nezbavuje.

Zpracovatel, stejně jako správce, musí být subjektem práva a nalézá se ve stavu podřízenosti vůči správci. Vztah se správcem musí být uzavřen smluvně a platí, že zpracovatelů pod jedním správcem může být několik. Pověřený zpracovatel pak může plnit i činnosti správce vůči subjektu údajů, jako je např. po-

skytování informací subjektu údajů. Zpracovatel je navíc povinen upozorňovat správce, pokud správce porušuje své povinnosti a v tom případě také musí zpracovatel zpracování údajů ukončit. V opačném případě je odpovědný za vzniklou škodu subjektu údajů stejným dílem jako správce. (Maštalka, 2008)

I přes absenci takového ustanovení v zákoně Úřad přijal výklad, že i pokud zpracování provádí zpracovatel, tak oznamovací povinnost plní vždy správce. (Matoušková a Hejlík, 2008)

3.3 Typologie osobních údajů

Dle Maštalky (2008) se můžou základní osobní údaje dělit do tří skupin podle toho, jak k nim subjekt údajů přišel. Patří mezi ně údaje:

- Přidělené pro obecnou identifikaci (jméno, příjmení, rodné číslo)
- Vrozené (otisk prstu, DNA, obličej)
- Přidělené pro určitý účel (adresa bydliště, telefonní číslo)

Matoušková a Hejlík (2008) pak rozdělují osobní údaje podle jejich typických vlastností na údaje identifikační, adresní, popisné a citlivé.

3.3.1 Identifikační údaje

Identifikační údaje jsou nejvíce univerzálně použitelnou skupinou údajů. Samy o sobě však často nemůžou sloužit k narušení soukromí. K tomu může dojít až při použití dalších, např. popisných nebo adresných, údajů, které jsou k identifikačním údajům navázány. Matoušová a Hejlík (2008) považují jako identifikační takový údaj, *„který lze použít k určení totožnosti subjektu v různých kontextech a za použití pouze dalších údajů plnících stejnou, tj. identifikační funkci a který se navíc vyskytuje v úředních záznamech.*“

- **Jméno a příjmení**

  Pojmy jméno a příjmení lze nalézt upraveny v § 61 – § 79 zákona č. 301/2000 Sb, o matrikách, jménu a příjmení. Každému občanovi se po narození zapíše jméno a příjmení do matriční knihy. Ze zásady se nesmí zapisovat jména zkomolená, jména opačného pohlaví a ani stejná křestní jména sourozencům společných rodičů. Povolené je pak používání dvou křestních jmen zároveň, viz Karel Hynek Mácha. Používání jména a příjmení je právem každého občana, zároveň má občan ale i povinnost ho používat před orgány veřejné moci. Právo na ochranu jména a příjmení má občan všude, kde jsou používány spolu s dalšími soukromými osobními údaji, až na výjimky stanovené zákonem. V případě, že člověk vstoupí do zaměstnání, je nevyhnutelné, aby používal svoje jméno a příjmení pro vnitřní komunikaci s ostatními lidmi v zaměstnání a případně za určitých zásad i pro komunikaci s veřejností. (Matoušková a Hejlík, 2008)

- **Datum a místo narození**

Stejně jako jméno, datum narození (přesněji den, měsíc a rok) se po narození člověka zapisují do matriční listiny a spolu s místem narození také do rodného listu. Slouží ve spojení se jménem k určení totožnosti a zůstávají po celý život nezměněny. Jediná změna může nastat přejmenováním místa narození, například dřívější název města Gottwaldov přejmenovaný na současný Zlín. (Matoušková a Hejlík, 2008)

- **Identifikační čísla**

  Pro určení totožnosti se dále používají identifikační čísla. V České republice k tomuto účelu slouží rodné číslo, případně pak daňové identifikační číslo, nebo číslo účtu u finanční instituce. Z rodného čísla, díky jeho vlastnostem sestavení, je možno zjistit datum narození dané osoby a její pohlaví. Z dalších osobních identifikačních čísel lze vybrat číslo občanského průkazu nebo cestovního pasu. Časem omezená platnost u těchto dokladů činí jejich identifikační čísla vhodná pro zpracování v oblasti osobních údajů. V rámci zaměstnání lze za identifikační číslo považovat i osobní číslo zaměstnance. Výhodou identifikačních čísel je, že podle něj lze přímo zjistit totožnost objektu, kterému je číslo přiřazeno. (Matoušková a Hejlík, 2008)

  Mates a spol. (2012) upozorňuje, že skladba rodného čísla se v historii měnila. Např. rodné čísla do konce roku 1953 měly místo dnešní čtyřmístné koncovky pouze koncovku trojmístnou. Podle počátečního čísla koncovky pak šlo poznat, zda se člověk narodil v Čechách, na Moravě či na Slovensku. Dodává také, že rodné číslo má vlastní právní úpravu, a to v zákoně č. 133/2000 Sb. o evidenci obyvatel a rodných čísel, ve znění pozdějších předpisů. Protože však tento zákon nebyl dostatečný z hlediska ochrany osobních údajů, byl v roce 2004 novelizován. Novela již obsahovala potřebné pravidla pro používání a využívání rodného čísla, a zároveň také sankce hrozící za porušení těchto pravidel.

3.3.2 Adresní údaje

Adresní údaje plní z podstaty dvě funkce. První je identifikační, kam lze zařadit údaje s vymezením především pro úřední potřebu. Patří sem např. adresa trvalého pobytu. Kontaktní funkce je daná tím, že je-li něco adresou, má smysl se tam obracet a někoho tam nalézt. (Matoušková a Hejlík, 2008)

- **Místní doručovací adresa**

  Za hlavní doručovací adresu se bere adresa trvalého pobytu. Tu může mít občan pouze jednu a obvykle ji má nahlášenou v místě, kde žije s rodinou, u rodičů nebo kde má byt. Adresa trvalého pobytu také slouží jako jeden ze základních identifikačních údajů. Další adresou může být adresa přechodného pobytu. Dříve měl občan zákonnou povinnost tuto adresu ohlásit, v současné době to je však na uvážení každého, zda jeho přechodnou adresu nahlásí. Jako adresa pro kontaktování a fyzické doručování může sloužit i adresa do zaměstnání. (Matoušková a Hejlík, 2008)

Dle § 29 odst. 1) písm. h) zákona č. 111/2009 Sb., o základních registrech se jako adresa považuje „*kombinace názvu okresu, názvu obce nebo vojenského újezdu, názvu části obce nebo v případě hlavního města Prahy názvu katastrálního území a názvu městského obvodu, čísla popisného nebo evidenčního, názvu ulice a čísla orientačního a dále zvláštních údajů pro doručování prostřednictvím poštovních služeb, která jednoznačně určuje adresní místo*“ (Zákon o základních registrech, 2009)

- **Účastnické adresy**

  Účastnické adresy nejsou, oproti předchozímu typu adres, vázané na fyzickou podstatu adresy, ale na účastnický vztah k poskytovateli služby. Hlavním zástupcem této skupiny je telefonní číslo (pevné domácí linky, soukromého či služebního mobilního telefonu, ale i linky do zaměstnání). Forma komunikace přes telefonní čísla je chráněna listovním tajemstvím stanoveným v čl. 13 LZPS. Do této kategorie patří i adresa elektronické pošty, tedy e-mail. I přes diskuze, zda e-mailová adresa je nebo není osobním údajem, by pro ni mělo platit, že je osobním údajem, pokud se dá prokázat objektivně existující vazba mezi touto adresou a subjektem údajů. (Matoušková a Hejlík, 2008)

3.3.3 Popisné údaje

Do kategorie popisných, neboli charakterizačních, údajů se zahrnují údaje, které utváří hlubší a ucelenější obraz subjektu údajů. Často se stává, že některé tyto údaje jsou vyžadovány i přesto, že pak nemají pro správce žádný účel. Stává se tak obvykle v případě, kdy zaměstnavatel převezme univerzální osobní dotazník a neupraví si ho v kontextu svých potřeb.

Popisné údaje lze dle Matouškové a Hejlíka (2008) dále rozdělit do dvou skupin na ty, které jsou:

- **Běžně užívané k identifikaci**

  Do této skupiny lze řadit ty popisné údaje úřední povahy, které mají spolu s identifikačními údaji rozlišovací schopnost a jsou tedy schopné plnit identifikační funkci. Nejrozšířenějším příkladem jsou akademické tituly, ať už před nebo za jménem. Jejich úmyslné neoprávněné užívání je přestupkem podle § 21 odst. 1 písm. d) zákona č. 200/1990 Sb., o přestupcích.

  Od 1.7.2017 vstoupí v účinnost zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, který nahrazuje zmíněný zákon č. 200/1990 Sb. o přestupcích. Tento zákon již neoprávněné užívání akademických titulů nezmiňuje. (Zákon o odpovědnosti za přestupky a řízení o nich, 2016)

- **Užívané k hodnocení subjektu údajů**

  Mezi popisné údaje užívané k hodnocení subjektu údajů lze zařadit například údaje o spotřebitelských zvycích, vykonávané profesi či údaje o trávení volného času. Takovéto údaje nemusí být přímo vyplněny či sděleny přímo

subjektem údajů, ale zpracovatel si je může generovat z kontextu chování daného subjektu údajů. (Matoušková a Hejlík, 2008)

3.3.4 Citlivé údaje

Citlivé údaje tvoří zvláštní okruh údajů mezi ostatními osobními údaji. Jednotlivé údaje, které do této kategorie patří, jsou taxativně uvedeny v § 4 písm. b) ZoOÚ (a mimo tyto vymezené údaje žádné jiné být označeny jako citlivé nemohou) a jejich ochrana má přísnější režim, než ostatní kategorie osobních údajů, viz § 9 ZoOÚ. Mezi tyto údaje patří např. údaje o národnostním, rasovém či etnickém původu, zdravotním stavu, náboženství, odsouzení za trestný čin (nikoliv pak pouhé jednání, které mohlo skončit odsouzením nebo pokuta za přestupek), sexuálním životě a orientaci a neposledně také genetické či biometrické údaje. Stejně jako u předchozích kategorií, i citlivé údaje musí být ve spojení s dalšími identifikátory, aby mohly za osobní údaje být brány. (Maštalka, 2008)

Matoušková a Hejlík (2008) dále uvádějí, že „*za údaje vypovídající o trestné činnosti je třeba považovat v prvé řadě údaje o osobách pravomocně odsouzených soudy České republiky, zaznamenané v evidenci Rejstříku trestů*“. Jsou tam založeny údaje identifikační o osobě odsouzeného, rozhodnutí o vině, trestu, ochranném opatření a jeho výkonu a případné dřívější propuštění z výkonu trestu. Dále je možné údaje vypovídající o trestné činnosti nalézt v opisech a výpisech z Rejstříku trestů.

- **Biometrické údaje**

  Biometrické údaje jsou vcelku novou záležitostí, což dokazuje i to, že nejsou zahrnuty v citlivých údajích ve Směrnici. V dnešní době se však stávají více a více užívanými a v rámci české legislativy už zahrnuty jsou. Aby mohl být brán biometrický údaj jako údaj citlivý, musí umožňovat přímou identifikaci subjektu údajů. Biometrická data lze rozdělit do dvou skupin. Zdrojem prvních jsou fyziologické vlastnosti člověka, kam patří DNA, otisky prstů, obraz sítnice či duhovky, a také rysy obličeje. V druhé skupině pak lze nalézt údaje založené na rysech chování či jednání. Patří tam např. vlastnoruční podpis nebo styl chůze. (Maštalka, 2008)

3.4 Úřad pro ochranu osobních údajů

Ať už podle Úmluvy č. 108 nebo Směrnice, v každém státě Evropské unie musí působit minimálně jeden orgán veřejné moci, který dohlíží na dodržování povinností pramenících ze zákona o ochraně osobních údajů. V České republice působí právě jeden takový orgán, Úřad pro ochranu osobních údajů (dále jen „Úřad“ nebo „ÚOOÚ“) se sídlem v Praze, nicméně lze nalézt i země jako Německo nebo Španělsko, kde je dozorových orgánů v oblasti ochrany osobních údajů více. Každý takový orgán plní dle terminologie Evropské unie kontrolní funkci. Tyto orgány tedy ze zásady musí být vybaveny pravomocemi, které jim dovolují shromažďovat informace potřebné pro plnění kontrolní funkce, pravomocí pro-

vádět šetření a pravomocí účinně zasáhnout a obrátit se na soud, pokud dojde k porušení zákona o ochraně osobních údajů. Vůči Úřadu mají občané právo obrátit se na něj s žádostí v oblasti zpracování údajů a Úřad má povinnost tuto osobu následně informovat o vyřízení její žádosti.

Úřad nepodléhá žádnému ministerstvu ani jinému státnímu orgánu, je plně nezávislým orgánem a řídí se pouze zákony. Díky tomu může a musí vykonávat dozor i u ostatních orgánů státní správy. (Matoušková a Hejlík, 2008)

V ustanoveních § 29 odst. 1 ZoOÚ lze nalézt vymezené úkoly, které Úřad plní:

a) *„Provádí dozor nad dodržováním povinností stanovených zákonem při zpracování osobních údajů*
b) *Vede registr zpracování osobních údajů*
c) *Přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování osobních údajů a informuje o jejich vyřízení*
d) *Zpracovává a veřejnosti zpřístupňuje výroční zprávu o své činnosti*
e) *Vykonává další působnosti stanovené mu zákonem,*
f) *Projednává přestupky a jiné správní delikty a uděluje pokuty podle tohoto zákona*
g) *Zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána, a z přímo použitelných předpisů Evropské unie*
h) *Poskytuje konzultace v oblasti ochrany osobních údajů*
i) *Spolupracuje s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů. Úřad v souladu s právem Evropské unie plní oznamovací povinnost vůči orgánům Evropské unie*“ (ZoOÚ, 2000)

3.4.1 Kontrolní činnost

Kontrolní činnost je první stěžejní činností Úřadu a provádějí ji inspektoři a další zaměstnanci Úřadu. Inspektorů je celkem 7 a jsou jmenováni prezidentem na základě návrhu Senátu Parlamentu České republiky. Kontroly můžou být prováděny na popud samotných občanů, ale i dle kontrolního plánu Úřadu. Při kontrole se musí kontrolor prokázat průkazem kontrolora, kontrolovanému subjektu oznámit zahájení kontroly a následně zachovávat mlčenlivost o skutečnostech, které při kontrole zjistil. Mlčenlivostí však samozřejmě není dotčena oznamovací povinnost, kterou kontrolující mají, nejčastěji v případu neoprávněného nakládání s osobními údaji. Výsledky kontroly musí být sepsané do kontrolního protokolu. Podrobnosti o tom, co musí protokol obsahovat lze nalézt v § 12 zákona č. 255/2012 Sb. o kontrole. Při kontrole jsou kontroloři oprávnění vstupovat do objektů kontrolovaného a požadovat předložení písemností, pokud to souvisí s předmětem kontroly, pořídit kopie obsahu paměťových médií, na kterých jsou osobní údaje uloženy a požadovat, aby v případě nedo-

statků kontrolovaní podali ve stanovené lhůtě písemnou zprávu o jejich nápravě. (Matoušková a Hejlík, 2008)

3.4.2 Vedení registru zpracování osobních údajů

V rámci registru zpracování osobních údajů, který Úřad vede na základě § 29 odst. 1 písm. b) ZoOÚ, Úřad udržuje oznámení přijaté od správců údajů, jež mají povinnost zaslat před počátkem zpracování údajů, za účelem získání přehledu o tom, kdo jaké údaje a jakým způsobem zpracovává. Nejedná se tedy pouze o soupis správců, kteří by mohli zpracovávat jakékoliv údaje. Úřad povoluje zpracování osobních údajů konkrétně podle jejich účelu, který by měl správce co nejpřesněji označit v registraci. Po oznámení musí Úřad vyrozumět správce do třiceti dnů, zda je registrace vyřízena. V případě, že to Úřad do třiceti dnů nestihne, má se podle zákona za to, že oznámení bylo zaregistrováno. Během zmíněných třiceti dní může Úřad kvůli neúplnému oznámení vyzvat správce, aby jej doplnil, případně opravil, nebo může zpracování nepovolit. (Vidrna a Koudelka, 2013)

Oznámení, které správce údajů musí doručit Úřadu, musí dle § 16 odst. 2 ZoOÚ obsahovat následující informace:

- *„a) identifikační údaje správce, u fyzické osoby, která není podnikatelem, jméno, popřípadě jména, příjmení, datum narození a adresu místa trvalého pobytu, u jiných subjektů obchodní firmu nebo název, sídlo a identifikační číslo osoby, pokud bylo přiděleno, a jméno, popřípadě jména, a příjmení osob, které jsou jejich statutárními zástupci,*
- *b) účel nebo účely zpracování,*
- *c) kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají,*
- *d) zdroje osobních údajů,*
- *e) popis způsobu zpracování osobních údajů,*
- *f) místo nebo místa zpracování osobních údajů,*
- *g) příjemce nebo kategorie příjemců,*
- *h) předpokládaná předání osobních údajů do jiných států,*
- *i) popis opatření k zajištění ochrany osobních údajů podle § 13.*“

3.5 Bezpečnost osobních údajů

Ne vždy byla chápána bezpečnost osobních údajů stejně jako dnes. V minulosti často docházelo redukování tohoto tématu pouze na ochranu bezpečnosti dat, která byla řešena pouze technickými prostředky, které data měly schraňovat proti neoprávněným přístupům. Pouhé technické řešení však nezaručí jejich dostatečnou aplikaci. Tento přístup nebyl v souladu s potřebou komplexní právní úpravy ochrany osobních údajů. V dnešním ZoOÚ již proto lze nalézt povinnost zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření, nikoli pouze technická. (Maštalka, 2008)

Ve Směrnici 95/46/ES (1995) se bezpečnosti osobních údajů věnuje čl. 17 odst. 1, ve kterém je uvedeno následující: „*Členské státy stanoví, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování. Tato opatření mají zajistit, s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny.*“

V ZoOÚ (2000) se bezpečnosti osobních údajů věnuje § 13, kde se v odst. 1 nachází následující: „*Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.*“

Maštalka (2008) dodává, že zmíněná směrnice a zákon ukládají v oblasti bezpečnosti osobních údajů jisté povinnosti, nicméně není nikde uvedeno, jakými prostředky a jakým způsobem by tyto povinnosti měly být splněny. Správce je nicméně zodpovědný pouze za ochranu před běžnými a rozumně předpokládanými riziky. Nelze tedy správcovy povinnosti zajištění ochrany považovat za absolutní. Takovou mimořádnou událostí byly například povodně v létě 2002, kdy došlo ke zničení několika databází s osobními údaji.

Pro vznik správního deliktu za porušení § 13 odst. 1 ZoOÚ nemusí ani dojít k neoprávněnému zpracování či zneužití osobních údajů. K naplnění skutkové podstaty stačí, aby došlo k určitému stavu ohrožení osobních údajů. Tím může být např. zasílání osobních údajů nechráněným e-mailem nebo neodbornou likvidací listin s osobními údaji, které se tak mohou dostat k neomezenému okruhu osob. (Pavlát, 2013)

V příručce vydané ÚOOÚ (2011) se nachází šest zásad, které by měly při zajištění bezpečnosti vždy platit:

- „*Spolehlivost – zajištění, že informace nebudou poskytovány nebo sdělovány neoprávněným osobám, nebudou dostupné pro nesouvisející zpracování*
- *Integrita – zajištění, že osobní údaje nebudou pozměněny nebo zlikvidovány neoprávněným způsobem*
- *Dostupnost – zajištění, že informace budou přístupné a bude možné je na požádání, na určitou dobu zpřístupnit oprávněným subjektem*
- *Odpovědnost – zajištění, že činnost subjektu může být jednoznačně přiřazena pouze danému subjektu*
- *Autentičnost – zajištění, že totožnost subjektu nebo zdroje je stejná jako ta, která je uvedena (autentičnost platí pro uživatele, procesy, systémy a informace)*

- *Nemožnost popření – zajištění nemožnosti popřít účast jakéhokoliv subjektu na změně osobních údajů*“

3.5.1 Organizační opatření

Každý obchodní závod by si měl provést vnitřní analýzu, aby dostal přehled o tom, jaká zpracování osobních údajů v jejich obchodním závodě probíhají a podle kterých právních předpisů se řídí. Získá tak informace o realizovaném zpracování i objektech, vůči kterým zpracování probíhá. Následně je třeba určit odpovědnosti lidem, či oddělením, za jednotlivé kroky zpracování osobních údajů. Mezi tyto kroky patří:

- vkládání a změna osobních údajů
- přístup k osobním údajům a jejich přenos
- technická podpora zpracování

Tímto krokem by se mělo zajistit, aby příslušné systémy nepoužívaly osoby, které k nim nemají mít přístup. Tématu omezení přístupu se více věnují odst. 3 a 4 § 13 ZoOÚ, kde je možné např. nalézt povinnost zabránit neoprávněnému čtení, kopírování, úpravě nebo mazání záznamů obsahujících osobní údaje, v oblasti automatizovaného zpracování pak povinnost pořizovat elektronické záznamy o vkládání či úpravách osobních údajů a další. Správné rozdělení pravomocí a přístupů k osobním údajům by mělo také pomoci k případnému určení osoby, která naruší integritu zpracování osobních údajů. (Maštalka, 2008)

Dále je dle Maštalky (2008) nutno kategorizovat bezpečnostní opatření do následujících třech kategorií:

- **Zajištění identifikace uživatelů**

  Zajištění identifikace uživatelů patří mezi nejzákladnější opatření pro zajištění bezpečnosti osobních údajů. Organizace musí mít vymezený jmenovitý seznam oprávněných osob, které mají přístup k určitým fázím zpracování osobních údajů, aby nedocházelo k neoprávněným přístupům a operacím s osobními daty.

  Jednodušší variantou se dají zmíněným způsobem ochránit data při automatizovaném zpracování. Pokud je bráno v potaz, že obchodní závod již má nějaký informační systém, stačí mu pouze pomocí nastavení oprávnění přidělit jednotlivým uživatelům úkony, které mohou provádět. Tímto krokem lze nastavit, že někteří uživatelé budou moci například jen prohlížet data, jiní je upravovat a někteří se k nim vůbec nedostanou. Samotnou identifikaci je pak možno řešit nutností přihlašování k počítači, respektive do informačního systému pomocí uživatelského jména a hesla.

  Složitějším případem je pak často manuální evidence. Opatření uvedená u automatizovaného zpracování, jako ochrana přístupu heslem, v tomto případě nelze použít a je třeba vybrat jiné. Jako jedna varianta se

nabízí uchovávání spisů s osobními údaji v trezoru, případně v uzamykatelných kartotékách.

- **Kontrola přístupu k zařízením a datům**

  Toto opatření, jak uvádí Maštalka (2008), je tvořeno především jako důsledné aplikování pravidel z předchozího bodu, tedy kontroly oprávněných přístupů k osobním údajům. Přidává však, že by měl existovat registr přístupů, ve kterém by se uchovávaly údaje důležité pro dohledání, kdo a jak s osobními údaji nakládal. Tato data by měla obsahovat identifikaci uživatele, čas ve který k přístupu došlo, k jakým souborům bylo přistupováno a informaci o provedených operacích.

  V případě přenosu osobních údajů po komunikačních sítích je pak třeba použít bezpečnostních mechanizmů, které data zašifrují tak, aby je během přenosu nemohl nikdo zachytit a přečíst, případně s nimi jinak manipulovat. Zajištěno musí být také dodání na správné místo.

- **Nastavení režimu nakládání s nosiči údajů**

  Oba předchozí body musí být podepřeny nastavením režimu nakládání s nosiči údajů. Mezi základní opatření lze považovat následující:

  - Zajištění popisu obsahu nosiče – pro identifikovatelnost informací na nosiči
  - Inventarizace nosičů – nosiče obsahující osobní údaje musí být uchovávány na místě, kam mají přístup pouze oprávněné osoby
  - Postup pro vyřazení opotřebených nosičů, který zajistí, aby z nich nemohly být znovu použity na nich uložené osobní údaje
  - Kontrola přístupu k osobním údajům, pokud jsou nosiče vynášeny z místa jejich obvyklého uchovávání

Maštalka (2008) dále dodává, že zvláště v případě zpracování citlivých údajů by mělo být požadováno, aby distribuce údajů být chráněna zašifrováním, či jakýmkoliv jiným mechanismem, který zabrání čitelnosti neautorizovaným osobám.

Dalším neméně důležitým opatřením pro udržení bezproblémového chodu, i během krizové situace, je vytváření zálohovacích kopií. Ty musí být pořizovány tak, aby byly prakticky využitelné a aby byly co nejlépe schopny obnovit data do původního stavu, který předcházel krizové situaci. Kopie by proto měly být na jiném místě, než kde probíhá vlastní zpracování osobních údajů. Důležité je i kopie průběžně kontrolovat a zastaralé likvidovat v souladu s povinností uchovávat pouze přesné osobní údaje.

Veškerá přijatá opatření by měla být sepsána do dokumentu, či dokumentů, s vymezením jejich rozsahu a dopadu. Takový dokument by podle Maštalky (2008) měl obsahovat následující:

- Rozsah působnosti zaváděného opatření

- Popis zaváděného opatření včetně dopadu na jednotlivé fáze zpracování osobních údajů
- Určení osob a jejich přístupů k jednotlivým prostředkům a způsobům zpracování osobních údajů
- V rámci určování totožnosti by měly být stanovené pravidla pro formu uživatelských hesel, včetně periodicity jejich povinné změny
- Pravidla pro pořizování zálohovacích kopií dat, jak často mají být zálohy vytvářeny a postup jak se budou osobní údaje v případě potřeby z těchto záloh obnovovat
- Pravidla pro práci s nosiči, tedy jejich používání, přenos a likvidaci

Jako poslední věc pak dodává, že s bezpečnostním opatřením ochrany osobních údajů by měli být seznámeni všichni zaměstnanci, a to nejen zpřístupněním výše popsaných dokumentů, ale i příslušným školením pro lepší pochopení práv a povinností v rámci ochrany osobních údajů.

3.6 Správní sankce při porušení zásad zpracování osobních údajů

Stejně jako u ostatních práv, právo na ochranu osobních údajů by nebylo bráno vážně, pokud by nebyly v zákonech zaneseny postihy za jeho porušení. Ochraně osobních údajů se věnuje mimo správního práva i právo trestní, nicméně jak uvádí Mates a spol. (2012), trestně mohou být stíhány orgány veřejné moci za prohřešky při zpracování osobních údajů v rámci výkonu veřejné moci, čímž se tato problematika dostává za hranice této práce a dále nebude rozváděna.

3.6.1 Přestupky

V oblasti ochrany osobních údajů je jednou ze základních povinností mlčenlivost. Tu musí dodržovat veškeré fyzické osoby, které přicházejí do styku s osobními údaji u správce nebo zpracovatele. Tato povinnost dle § 15 odst. 1 ZoOÚ trvá i mimo dobu pracovního poměru (respektive na základě dohody, pracovní poměr není nutný) a není časově ohraničena. Porušením této povinnosti se fyzická osoba dopouští přestupku dle § 44 odst. 1 ZoOÚ a hrozí ji pokuta do výše 100 000 Kč. (Kolman, 2010)

V dalším okruhu přestupků dle § 44 odst. 2 ZoOÚ, ve kterých lze uložit pokutu do výše 1 000 000 Kč, lze nalézt pochybení v nestanovení účelu, prostředků nebo způsobu zpracování osobních údajů. Případně porušení povinnosti nebo překročení oprávnění při stanovení účelu zpracování. Jako další skutkovou podstatu je možné uvést zpracovávání nepřesných osobních údajů, jelikož dle zákona č. 101/2002 Sb., o ochraně osobních údajů je nutné zpracovávat pouze přesné osobní údaje. Při zjištění správce, že zpracované údaje nejsou přesné, musí být bez zbytečného odkladu zablokováno zpracování postižených údajů. Tím se rozumí na určitou dobu znepřístupnit daný osobní údaj, aby bylo zabráněno jeho zpracování, jak je uvedeno v §4 ZoOÚ písm. h). Pokud nedojde

k opravě či doplnění údajů, má správce povinnost tyto osobní údaje zlikvidovat. Mezi další skutkové podstaty v tomto okruhu přestupků patří uchovávání osobních údajů po delší než nezbytnou dobu, která je nutná k účelu jejich zpracování (po této době je možné uchovávat dané údaje v anonymizované formě např. pro účely státní statistické služby), zpracovávání údajů bez souhlasu subjektu údajů, neposkytnutí či odmítnutí předání informací subjektu údajů na základě § 12 a 21 ZoOÚ, nebo nesplnění oznamovací povinnosti dle ustanovení § 16 ZoOÚ. Od 1. dubna 2009 se mezi přestupky s hranicí pokuty do 1 000 000 Kč stalo také porušení zákazu zveřejnění osobních údajů dle § 44a ZoOÚ. Zmíněných správních deliktů se může dopustit pouze správce nebo zpracovatel.

Za nejzávažnější správní delikty pak lze považovat podle § 44 odst. 3 ZoOÚ ohrožení většího počtu osob neoprávněným zasahováním do soukromého a osobního života (pomocí skutků v předcházejících odstavcích) a porušení povinnosti pro zpracovávání citlivých údajů, které je z jejich podstaty důležitější chránit. Zároveň sem také patří porušení dle § 44a ZoOÚ, zmíněného v předchozím odstavci, pokud byl přestupek spáchaný tiskem, televizí nebo obdobně účinným způsobem. Zmíněných deliktů se opět může dopustit pouze fyzická osoba v roli správce nebo zpracovatele, kterým může za výše uvedené skutky být udělena pokuta do výše 5 000 000 Kč. (Kolman, 2010)

K maximální výši pokuty se však přistupuje pouze v mimořádných případech. Výši pokuty určuje ÚOOÚ podle závažnosti, doby trvání, vzniklých následcích a dalších okolností, které protiprávní jednání doprovázely. U případů, kdy není přestupek spáchán z nedbalosti, ale úmyslně, je zpravidla uložena vyšší pokuta. Splatnost pokuty je pak 30 kalendářních dnů ode dne, kdy uložení pokuty nabylo právní moci. Výtěžek z těchto pokut putuje do státního rozpočtu. (Mates a spol., 2012)

3.6.2 Jiné správní delikty

Jiných správních deliktů se dle §45 ZoOÚ může dopustit jak podnikající fyzická osoba, tak i osoba právnická. Oproti přestupkům v §44 ZoOÚ jsou v této kategorii vyšší sankce. Méně závažný jiný správní delikt (dle § 45 odst. 1 ZoOÚ) lze pokutovat do výše 5 000 000 Kč, společensky závažnější jiné správní delikty (dle § 45 odst. 2 ZoOÚ) pak sazbou až do výše 10 000 000 Kč. Obdobně jako u přestupků vstoupil v účinnost od 1. dubna 2009 nový § 45a ZoOÚ, dle kterého se správním deliktem stalo zveřejnění osobních údajů stanovených jiným právním předpisem. Zde zůstaly stejné maximální výše pokut jako u přestupků, a to 1 000 000 Kč pro méně závažné provinění (dle odst. 1) a 5 000 000 Kč za více závažné provinění (dle odst. 2). (Kolman, 2010)

Odpovědnost právnické osoby je časově ohraničená a zaniká rok po nahlášení jiného správního deliktu, pokud příslušný správní orgán do zmíněné doby nezahájil řízení. Každý jiný správní delikt musí být nahlášen a pravomocně rozhodnut nejpozději do tří let ode dne jeho spáchání. (Mates a spol., 2012)

3.6.3 Pořádkové delikty

Skutková podstata pořádkových deliktů spočívá v maření průběhu dozoru Úřadu. Provinit se může fyzická osoba tím, že nespolupracuje s Úřadem, např. nevydá dokumenty potřebné pro provedení kontroly Úřadem. Hranice sankce pro pořádkové delikty je 25 000 Kč a může být udělována opakovaně, dokud nedojde k nápravě. (Mates a spol., 2012)

3.7 Soukromí

Pojem soukromí, respektive právo na soukromí, je zejména poslední dobou velmi často používaným pojmem. Každý si pod pojmem soukromí něco představí a zdánlivě mu rozumí. Pokud se však dostane do situace, kdy má vysvětlit, co soukromí znamená, neví jak tento pojem vysvětlit. Podobně tomu však je i v právních dokumentech. Právo soukromí ochraňuje, nicméně přímo pojem soukromí nelze nikde najít právně definovaný, ať už v právu českém, evropském či mezinárodním. (Fialová, 2016)

Teoretických definic pojmu soukromí je však velké množství. Warren a Brandeis (1890) již v roce 1890 publikovali názor, že právo na soukromí by mělo znamenat *„právo být ponechán o samotě (right to be let alone)*“. Právo na soukromí mělo člověka dle jejich smýšlení ochránit před novými technologickými vynálezy a obchodními praktikami, které zasahovaly do osobního a rodinného života.

Westin (1967) pak v 60. letech 19. st. chápal soukromí jako právo člověka, ale i instituce nebo skupiny, na rozhodnutí, kde a v jakém rozsahu budou informace o jeho osobě sdíleny ostatním. Soukromí jednotlivce pak vysvětloval jako odchod člověka ze společnosti do samoty, malé skupiny, či anonymity ve větší skupině.

Zajímavý názor přináší i Sobek (2011), který uvádí, že právo na soukromí může být realizováno i prostřednictvím zveřejnění informací o sobě. Pokud by měl člověk zakázáno tyto informace zveřejňovat, mohlo by to být považováno za zásah do soukromí člověka. Souhlasí tím i s názorem Westina, tedy že by člověk měl mít vlastní kontrolu nad osobními informacemi.

Barendt (2006) bere soukromí jako vlastní volbu, které údaje o sobě chceme nechat anonymní. Jako příklad uvádí telefoní číslo, kdy si ho mnozí snaží chránit v anonymitě, aby jim nepřicházely marketingové telefonáty. Podobně pak vidí zacházení s e-mailovými adresami. Tyto příklady specifičtěji pojmenovává jako pozoronostní soukromí.

Jako relativní pojem vidí soukromí Gutwirth (2002), který říká, že chápání soukromí se historicky vyvíjelo a je v různých zemích různě chápáno na základě historických, společenských, kulturních a náboženských podmínek. V řecko-římském starověku bylo soukromí chápáno jako něco negativního a člověk, který se odebral do soukromí, nebyl brán o nic lépe než otrok. V dnešním kontextu je soukromí západní civilizace spjato s demokratickým státem, individualismem a nezávislostí chování jednotlivce.

V rámci české judikatury se český Ústavní soud k pojmu soukromí vyjádřil v nálezu II. ÚS 517/99 ze dne 1. 3. 2000, kde vymezil soukromí jako *„právo fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob s rovným právním postavením“*.

3.7.1 Právní ochrana soukromí

I s přihlédnutím k faktu, že neexistuje žádná legální definice soukromí, právo na ochranu soukromí je obsaženo ve vícero dokumentech. Jako první je možno uvést čl. 12 ve Všeobecné deklaraci lidských práv (dále jen VDLP) z roku 1948 a dále např. Mezinárodní pakt o občanských a politických právech z roku 1966, který byl VDLP inspirován. (Fialová, 2016)

V rámci Evropy je pak nejdůležitějším dokumentem, týkajícím se ochrany soukromí, Evropská úmluva o lidských právech a základních svobodách (dále jen EÚLP) z roku 1950, kde je právo na respektování soukromého života zakotveno v čl. 8. takto:

1. *„Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.“*
2. *„Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.“*

V případě, že smluvní stát poruší vůči jednotlivci právo na soukromí, může se poškozený dovolávat svého práva u Evropského soudu pro lidská práva. Ten posuzuje, zda došlo k porušení práv dle čl. 8 EÚLP, ve čtyřech krocích. Nejdříve je zkoumáno, jestli vůbec k porušení práv, tedy zásahu do soukromí, došlo. Takovým zásahem do práv může být např. tajný dohled nad telefonickou komunikací či sledování člověka pomocí technologie GPS. Pokud k zásahu do soukromí došlo, soud přezkoumá, zda k tomu nedošlo na základě nějakého soudního rozhodnutí. V rámci třetího kroku soud zkoumá, zda je omezení práva na soukromí v souladu s druhým odstavcem čl. 8 EÚLP. Soudu však k rozhodnutí nestačí pouhé určení legitimního cíle podle výjimek uvedených v druhém odstavci čl. 8 EÚLP, a tak ještě musí zvážit, zda je splněna další podmínka ze zmiňovaného odstavce, tedy zda je omezení práva na soukromí nezbytné v demokratické společnosti. (Fialová, 2016)

Také v českém právním řádu je ochrana soukromí zakotvena v Listině základních práv a svobod (dále jen LZPS). Zakotvenou ji lze nalézt ve více článcích zároveň. V rámci čl. 7 odst. 1 LZPS je zaručeno samotné právo na soukromí s dodatkem, že v případech stanovených zákonem může být omezena. Ochranu před neoprávněným zasahováním do soukromého a rodinného života se pak nachází v čl. 10 odst. 2 LZPS. Jako respektování ochrany soukromí lze také brát

garanci nedotknutelnosti obydlí zakotvenou v čl. 12 LZPS a uchovávání listovního tajemství, tajemství zpráv podávaných telefonem a dalších tajemství jiných písemností a záznamů zakotveného v čl. 13 LZPS (LZPS, 1992)

Právo na soukromí lze nalézt zanesené i v občanském zákoníku v rámci soukromého práva. Při nahlédnutí do § 3 odst. 1 OZ lze nalézt definici: „*Soukromé právo chrání důstojnost a svobodu člověka i jeho přirozené právo brát se o vlastní štěstí a štěstí jeho rodiny nebo lidí jemu blízkých takovým způsobem, jenž nepůsobí bezdůvodně újmu druhým.*“ Ve druhém odstavci zmíněného paragrafu se pak nachází zásady, na kterých soukromé právo spočívá a právě mezi nimi se nachází právo na soukromí, na stejné úrovni s právem na ochranu svého života, svobody, cti a důstojnosti. Dále lze právo na soukromí nalézt v § 81 OZ, který se věnuje ochraně osobnosti. Podrobněji rozepsané právo na soukromí lze nalézt v § 86 OZ: „*Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.*“

3.7.2 Ochrana soukromí zaměstnance na pracovišti

V rámci pracovněprávních vztahů je ochrana soukromí zaměstnance zanesena v § 316 odst. 2 ZPr, ve kterém se lze dočíst následující: „*Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.*“

Za zvláštní povahu činnosti zaměstnavatele Vidrna a Koudelka (2013) považuje takové pracoviště, kde se může proběhnout zpronevěra velkých finančních částek, může dojít ke škodě na majetku značného rozsahu nebo k ohrožení na životě. § 316 odst. 2 ZPr je kogentní normou a zaměstnavatel ji proto nemůže obejít ani případným souhlasem zaměstnance.

V rámci ústavního řádu má každý zaměstnanec právo na uspokojivé pracovní prostředí, které mimo jiné věci zahrnuje i limity pro zásahy do soukromí. Zaměstnanec má právo na rozvíjení soukromého života i v rámci výkonu práce, neboť oddělit přesně soukromý a pracovní život není lehké. Hlavní zásadou pracovněprávního vztahu je však skutečnost, že zaměstnanec by měl trávit veškerou pracovní dobu výkonem práce. Aktivity vykazující soukromou povahu může zaměstnanec provozovat, pokud je to nezbytné, nebo pokud to má povoleno od zaměstnavatele. Podle práva si ale zaměstnanec nemůže bez svolení vyplňovat pracovní dobu volnočasovými soukromými aktivitami, když mu zrovna není přidělená práce. Zaměstnavatel má pravomoc přiměřeným způsobem zmíněné podmínky kontrolovat a chránit si tím svůj majetek. Nastává zde tedy otázka,

jaká je hranice mezi zaměstnancovým právem na soukromí a zaměstnavatelovým právem na ochranu jeho majetku.

Konfliktem mezi právem na soukromí a ochranu osobních údajů zaměstnance, které patří mezi základní lidská práva, vůči vlastnickému právu na ochranu zaměstnavatelova majetku se věnuje test proporcionality. Test proporcionality je metodou, která zkoumá v případě konfliktu základních práv a svobod přiměřenost daného konfliktu. (Morávek, 2013)

Ústavní soud v nálezu Pl.ÚS 4/94 ze dne 12. 10. 1994 vyčlenil tři základní podmínky, za kterých může být jedno základní právo omezeno ve prospěch jiného základního práva. U každé činnosti způsobující zmíněný konflikt se zkoumá, zda pro naplnění jejího cíle, tedy ochrany jiného základního práva, splňuje následující:

- Je vhodná, čím je myšleno, že lze zvoleného cíle dosáhnout.
- Je potřebná, tedy nelze pro naplnění cíle využít jiného řešení, které by zasahovalo do chráněných zásad méně nebo vůbec.
- Je přiměřená v užším slova smyslu, tedy že prospěch ze zkoumané činnosti způsobující konflikt je větší než škoda způsobená touto činností. V potaz se berou empirické, systémové, kontextové a hodnotové argumenty.

Morávek (2013) dodává, že v rámci LZPS jsou si veškerá práva a svobody rovny. V praxi však, pokud dojde ke kolizi dvou základních lidských práv či svobod, jedno z nich musí být na úkor druhého upřednostněno. Dodává také, že test proporcionality však ještě stále není ustálen do konečné formální podoby.

3.8 Monitorování zaměstnanců

Informační a komunikační technologie, díky kterým je možné monitorovat aktivitu zaměstnanců a tím porušovat jejich soukromí, prošly za posledních pár let velkým a významným technologickým vývojem a jsou dnes velmi rozšířené a relativně levně dostupné. Oproti tomu zákony na ochranu soukromí za posledního půl století žádnou velkou změnou neprošly. To představuje mnohá rizika v oblasti ochrany lidských práv a svobod. Díky novým technologiím jsou v určitých případech zmenšovány rozdíly mezi pracovní dobou a soukromým životem. Mezi takové patří např. práce z domu či povinnost být dosažitelný na telefonu, tedy práce na zavolání. V oblasti kontroly pak zaměstnavatele můžou nově dostupné technologie vést ke kontrolování elektronické pošty, využívání internetu zaměstnanci během pracovní doby, kontrole obsahu hovorů uskutečněných pomocí služebních telefonů a dalších. (Bartík a Janečková, 2016)

3.8.1 Kamerové systémy

Pomocí kamerových systémů jsou lidé sledováni v reálném čase. Na straně sledovaných, v našem případě zaměstnanců, mohou vyvěrat obavy z omezování soukromí. Na opačné straně, v našem případě zaměstnavatelů, je to nástroj, který účinně umožňuje odhalovat kriminalitu páchanou na zaměstnatelově majetku

i jiné trestné činnosti. Kromě ochrany majetku je pak kamerový systém účinný i pro kontrolu zaměstnanců, zda poctivě pracují po celou dobu jejich pracovní doby. Pro obě strany pak může kladně působit tím, že pomáhá obecně udržovat bezpečnostní situaci osob i majetku na pracovišti. (Bartík a Janečková, 2016)

V České republice prozatím neexistuje zákon, který by se kamerovým systémům primárně věnoval. V současné době se tedy kamerové systémy řídí zákoníkem práce a ZoOÚ. Ne pokaždé lze ale ke kamerovým systémům vztahovat oba zákony. Je nutné rozdělit kamerové systémy do dvou skupin podle toho, zda ukládají nebo neukládají kamerový záznam. (Janečková, 2014)

V případě kamerového systému, který videozáznam neukládá, se dle ZoOÚ nejedná o zpracování osobních údajů. Vůči dalším předpisům však může i tato verze kamerového systému být v rozporu. V oblasti pracovněprávních vztahů lze hlavně uvést potenciální narušení již dříve zmiňovaného § 316 odst. 2 ZPr, ve kterém je zaměstnanci zaručeno, že zaměstnavatel nebude narušovat jeho soukromí otevřeným či skrytý sledováním. Aby zaměstnavatel mohl kamerový systém používat, je nutné, aby pracoviště splňovalo podmínku zvláštní povahy činnosti, která je také uvedena v § 316 odst. 2 ZPr. Pokud zaměstnavatel tuto výjimku využije, musí pak dle § 316 odst. 3 ZPr zaměstnance přímo informovat o rozsahu kontroly a způsobu jejího provádění.

Význam kamerových systémů bez ukládaného videozáznamu je možné nalézt v případech, kdy je zapotřebí zásah osob v reálném čase. Jako příklad lze uvést zdravotnická zařízení, sociální ústavy pro malé děti, řízení letového provozu či jadernou elektrárnu. (Vidrna a Koudelka, 2013)

Provozování kamerových systémů s ukládaným záznamem již legislativně patří do zpracování osobních údajů, jelikož ze záznamu lze identifikovat subjekt údajů. Janečková (2013) tuto kategorii kamerových systémů definuje jako „*automaticky provozovaný stálý technický systém umožňující pořizovat a uchovávat zvukové, obrazové nebo jiné záznamy ze sledovaných míst a to např. formou pasivního monitorování prostoru nebo pořizování cílených záběrů (zachycování pohybu)*“.

V rámci oznámení Úřadu musí správce uvést umístění kamer, adresy míst uložení a zpracování záznamu, počet instalovaných kamer, popis záběrů kamer a technické řešení těchto kamer. Kromě oznámení je nutné dále zpracovávat dokumentaci týkající se informací o tom, kdo měl přístup ke kamerovým záznamům, komu byly předány a informace o provozních událostech. Dále je pak nutné vyvěsit v místech před vstupem do sledovaných prostor nepřehlédnutelné informační cedule s piktogramem o provozování kamerového systému a kontaktem, kam je možné se obrátit pro více informací o používaném kamerovém systému. (ÚOOÚ, 2012)

Samotná registrace však není povolovacím procesem, ale slouží pouze k povinnému oznámení Úřadu. Zda je zpracování údajů skutečně v souladu se zákonem lze posoudit až po kontrolním řízení provedeném na místě pracoviště. (Bartík, 2010)

Ombudsman Varvařovský (2011) však upozorňuje na pokulhávání zákona za technologiemi. V dnešní době jsou technologické řešení kamerových systémů

na úrovni, která dovoluje přepnout z režimu bez záznamu do režimu se záznamem jediným kliknutím, díky čemuž se mnozí zaměstnavatelé mohou vyhýbat povinnostem dle ZoOÚ a kličkovat tak na pomezí zákona.

Janečková (2014) dodává, že i pokud využije zaměstnavatel výjimku uvedenou v § 316 odst. 2 ZPr o povaze zvláštní činnosti a kamerový systém (ať už se záznamem, nebo bez) provozuje, nesmí ho používat pro monitorování zaměstnanců bez omezení. Zaměstnavatel nesmí umístit kamery do míst určených pro ryze soukromé potřeby, jako je např. toaleta, šatna nebo místa určená k odpočinku.

3.8.2 Přístup na internet

Zaměstnavatel by měl jasně vymezit, např v pracovním řádu nebo pracovní smlouvě, jak mohou zaměstnanci zacházet s internetem během pracovní doby. Zda ho mohou vůbec využívat pro osobní účely, a pokud ano, tak v jaké míře. V případě jakýchkoliv omezení by měl zaměstnavatel v rámci plnění druhé podmínky testu proporcionality, místo monitorování zaměstnaneckých aktivit na internetu, technicky znemožnit přístup na jiné stránky, než které zaměstnanci potřebují k výkonu práce. Toto opatření však může být leckdy i nemožné, pokud zaměstnanec musí pracovat s internetem a není tak možno určit, které stránky s jeho pracovním výkonem budou souviset. Naopak ale může zaměstnavatel blokovat určité stránky, které nechce, aby zaměstnanci navštěvovali.

Zaměstnavatel také může kontrolovat přístupy k internetu z jeho firemní sítě anonymně, tedy bez identifikace těchto přístupů. V případě že uzná, že zaměstnanci pravděpodobně tráví příliš mnoho času soukromě na internetu, může přistoupit k hlubší kontrole, která spojí přístupy s fyzickými osobami. Během kontroly lze zjistit čas, dobu trvání přístupu a míru aktivity na webových stránkách. Zaměstnavatel by měl tuto kontrolu provádět hlavně u webových stránek, které zaměstnanec s jistotou nepoužívá pro pracovní výkon. Takové kontroly jsou pak zcela legitimní v rámci práva zaměstnavatele kontrolovat plnění povinností zaměstnanců, které vyplývají z pracovněprávního vztahu.

Při porušení předem daných podmínek zaměstnancem má zaměstnavatel právo provést příslušné sankční postihy nabízené ZPr. (Morávek, 2013)

Pravomoc zaměstnavatele ke kontrole pohybu zaměstnanců na internetu stvrdil i Nejvyšší soud České republiky v judikátu 21 Cdo 1771/2011. Zaměstnanec v tomto případě využíval internet během pracovní doby pro svou potřebu, i přes striktní zákaz zaměstnavatele. Zaměstnanci byl na základě hrubého porušení pracovní kázně ihned ukončen pracovní poměr, proti čemuž se zaměstnanec obrátil na soud s připomínkou, že zaměstnavatel porušil § 316 odst. 3 ZPr, tedy tajně sledoval užívání internetu. Soud však dal za pravdu zaměstnavateli, protože přiměřená kontrola zákazu používání internetu pro soukromé účely je jasně uvedena v § 316 odst. 1 ZPr.

3.8.3 E-mailová pošta zaměstnanců

Stejně jako u přístupu k internetu platí u firemní e-mailové korespondence to, že pokud zaměstnavatel výslovně nesvolí k jejímu soukromému používání, nemá zaměstnanec právo soukromou korespondenci na pracovišti řešit. Morávek (2013) z tohoto také vyvozuje, že každý e-mail, který dorazí na pracoviště je pracovní, pokud není důvod domnívat se jinak.

Do pracovní korespondence zaměstnance má zaměstnavatel právo nahlížet. Jedním z důvodů, proč by mohl zaměstnavatel číst zaměstnancovu korespondenci, je ochrana svého majetku díky prodlevě způsobené zaměstnancovou nepřítomností např. z důvodu nemoci, nebo kontrola využití pracovní doby. Pokud je však zřejmé, že korespondence je soukromá (podle odesílatele, předmětu nebo oslovení), zaměstnavatel tuto poštu číst nesmí, neboť by porušil listovní tajemství zakotvené v čl. 13 LZPS. Je nezbytné brát v potaz, že i elektronická pošta je ve smyslu práva chápana jako pošta a elektronické písemnosti jako písemnosti. (Morávek, 2013)

Bartík a Janečková (2016) dodávají, že listovní tajemství je také zaručeno v rámci § 182 trestního zákoníku a §81 OZ. Dále uvádějí, že dodržování pracovní doby a jejího využití a získávání pracovních informací v době zaměstnancovy nepřítomnosti nejsou jediné aktivity, proč by odůvodněně mohl zaměstnavatel kontrolovat zaměstnancovu korespondenci. Jako další uvádí *„síťovou bezpečnost, povinnost předcházet a chránit zaměstnance před různými formami obtěžování, ochranu obchodního tajemství, ochranu před nedovoleným kopírováním dat a filtrování spamu*“. Stejně jako v předchozích případech by správně měl zaměstnavatel oznámit tyto kontroly zaměstnancům v rámci pracovní smlouvy nebo pracovního řádu. Dodávají také, že nelze v žádném případě akceptovat trvalé monitorování korespondence zaměstnanců. Zaměstnavatelům musí stačit kontrola namátková.

3.8.4 Služební telefony

Mezi služební telefony se řadí jak pevné linky, tak i telefony mobilní. V praxi je běžné, že zaměstnavatel dovoluje zaměstnancům využívat služební telefon i pro soukromé hovory. Pravidlem však bývá, že zaměstnanec musí soukromé hovory od pracovních odlišit, aby mu mohly být zaměstnavatelem vyúčtovány. Řešit se to dá např. stisknutím * (hvězdičky) před vytočením požadovaného čísla. Zda zaměstnanec toto pravidlo dodržuje, může zaměstnavatel namátkově kontrolovat. Zaměstnanec na vyžádání musí sdělit u vybraných pracovních hovorů informaci o tom, kdo byla volaná osoba. V případě odhalení nenahlášeného soukromého hovoru mezi pracovními může být zaměstnanec patřičně postihnut za porušení pracovní kázně. Stejně tak může být postihnut, i pokud odmítne sdělit identitu volané osoby. (Bartík a Janečková, 2016)

Podle § 250 odst. 1 ZPr je zaměstnanec *„povinen nahradit zaměstnavateli škodu, kterou mu způsobil zaviněným porušením povinností při plnění pra-*

covních úkolů nebo v přímé souvislosti s ním“. V tomto případě tedy uhradit telefonní poplatky.

LZPS a trestní zákoník zaručuje, že obsahy telefonních hovorů podléhají ochraně proti odposlouchávání. Zaměstnavatel tedy nemůže pořizovat záznamy obsahu jednotlivých hovorů.

Kontrola hovorů by měla mít namátkovou podobu. V případě, že zaměstnavatel systematicky a průběžně vede záznamy o tom, kolik daný zaměstnanec učiní soukromých hovorů, jejich délku a volané číslo, se již bude jednat o zpracování osobních údajů dle § 4 písm. e) ZoOÚ. Takové zaznamenávání je však v pořádku s právním řádem. Využívá totiž výjimky §5 odst. 2 písm. a) ZoOÚ, tedy nezbytné zpracování osobních údajů bez souhlasu subjektu nutné pro plnění právní povinnosti, kterou se v tomto případě myslí uchovávání faktur za telefonní hovory pro účely účetnictví. (Bartík a Janečková, 2016)

3.8.5 Služební automobily

Výrazně nákladnějším, oproti mobilním telefonům, jsou právě služební automobily, a proto by mělo být v zaměstnavatelově zájmu využívání tohoto prostředku efektivně kontrolovat. Díky technologii GPS fungující na bázi satelitů lze pozorovat, kde se daný automobil nachází v danou chvíli, ale i zpětně prohlédnout celou trasu jízdy. Odhaduje se, že takové zařízení má již více než polovina firemních automobilů. (Bartík a Janečková, 2016)

Oprávněnost použití technologie GPS není jednoznačná pro všechny typy zaměstnání. Zaměstnavatel ji stejně jako v předchozích případech musí použít za účelem ochrany majetku, dodržování pracovněprávních předpisů a podobně. S naprostou jistotou je vhodné například pro společnosti zařizující kamionovou dopravu, která díky záznamům z GPS může kontrolovat plnění povinných přestávek zaměstnanců nebo plnění naplánovaných tras. Jako nepřiměřenou pak lze považovat kontrolu pomocí GPS, když je zaměstnanec jednou za čas vyslán na kratší jízdu, např. za klientem, s využitím firemního automobilu. (Kadlecová, 2015)

Pokud jsou v rámci GPS systému zpracovávány systematicky pouze nezbytná data, např. o počtu najetých kilometrů, není zaměstnavatel povinen od zaměstnance vyžádat souhlas v souladu s § 5 odst. 2 písm. e) ZoOÚ, ale musí ho o shromažďování zmíněných dat informovat. Mnozí zaměstnanci měli tendence tomuto shromažďování dat zamezovat různými způsoby, např. zastíněním GPS přijímače alobalem, aby mohli využívat automobil pro svou potřebu. Moderní systémy však takovou manipulaci dokáží rozpoznat a uložit o tom informaci do své paměti. (Bartík a Janečková, 2016)

Kadlecová (2015) dodává, že z důvodu obsáhlosti informací, které musí být dle ZoOÚ zpracovány z informační povinnosti, je vhodné tuto povinnost vyřešit začleněním do interního předpisu obchodního závodu.

Mnozí zaměstnavatelé poskytují služební automobily i k soukromým účelům. V takovém případě by měl mít GPS systém v automobilu mít možnost nastavit minimálně dva režimy. Jeden pro firemní a druhý pro soukromé jízdy, aby

nedocházelo k monitorování zaměstnance ve chvílích, kdy nevykonává pracovní povinnosti. Takové monitorování by porušovalo zaměstnancovo právo na soukromí. (Kadlecová, 2015)

3.9 Nové obecné nařízení o ochraně osobních údajů (GDPR)

Hlavním evropským dokumentem pro zacházení s osobními údaji je nyní Směrnice 95/46/EC, která ukládá stejné práva a povinnosti jak pro papírové zpracování dat, tak i pro řešení v počítači či na cloudu. Je tomu tak z důvodu, že v roce 1995, kdy byla Směrnice 95/46/EC vydaná, neexistovaly ještě mnohé technologie, které jsou dnes běžně dostupné (např. cloudové úložiště a sociální sítě) a tak jimi není Směrnice 95/46/EC dostatečně regulována. (Bartolini et al., 2015)

Burian a Radičová (2016) jako důvod dnešní nedostatečnosti Směrnice 95/46/EC udávají nejen technologický pokrok, ale také to, že 28 různých zemí v rámci Evropské unie tuto směrnici transponovalo do své legislativy a vzniklo tak 28 různých národních předpisů týkajících se ochrany osobních údajů, což přináší problémy společnostem podnikajícím v celosvětovém měřítku, jenž musí veškerou legislativu daných států dodržovat.

V rámci České republiky se ochraně osobních údajů věnuje zákon č. 101/2000 Sb., o ochraně osobních údajů, který stejně jako Směrnice 95/46/EC současnému vývoji technologií nestačí. Evropský parlament proto schválil dne 27. dubna 2016 nové Obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation, dále jen GDPR) s účinností stanovenou na 25. května 2018. Toto nařízení nahradí Směrnici 95/46/EC, a protože nařízení je závazné bez nutnosti začlenění do národní legislativy, nahradí i ZoOÚ (nemusí být nutně zrušen v případě, že dojde k jeho novelizaci). GDPR nicméně dovoluje členským státům odchýlení od některých ustanovení. Novinkou je fakt, že působnost GDPR se nevztahuje pouze na správce a zpracovatele v rámci Evropské unie, ale i na všechny ostatní společnosti, které zpracovávají osobní údaje spotřebitelů v Evropské unii např. za účelem marketingu, prodejních aktivit a podobně. Cílem GDPR je pak jednotná úroveň ochrany fyzických osob a důrazné vymáhání práva. (Hrdlík, 2016)

Od přijetí GDPR začal Úřad pro ochranu osobních údajů poskytovat konzultace o, především praktických, dopadech GDPR na správce a zpracovatele údajů. ÚOOÚ je také společně s dalšími součástí vládní skupiny, která projednává problematiku a dopady GDPR (Paták, 2016)

3.9.1 Práva subjektů údajů

GDPR kromě stávajících práv subjektů údajů přináší následující čtyři nová práva (Dušek, 2017):

- Právo na výmaz – právo být zapomenut; pokud správci nesvědčí žádný zákonný titul pro zpracování, má povinnost na základě požadavku subjektu údajů vymazat jeho osobní údaje

- Právo na přenositelnost údajů – předání osobních údajů od jednoho správce druhému za podmínky technické proveditelnosti
- Právo vznést námitku – proti zpracování a tím omezit zpracování osobních údajů v případě, kdy subjekt údajů nemá dostatečné právo pro výmaz
- Právo na lidský zásah v případě rozhodnutí na bázi automatizovaného zpracování a profilování – subjekt údajů může vyjádřit názor a napadnout rozhodnutí

3.9.2 Povinnosti správců a zpracovatelů

Termíny správce a zpracovatel zůstávají v nové GDPR stejně definované jako ve Směrnici 95/46/EC, nicméně jejich povinnosti se mění. První zásadní změnou je upuštění od oznamovací povinnosti správce, kdy má správce povinnost oznámit dozorovému orgánu (v naší republice je tímto orgánem ÚOOÚ) zpracování údajů před jeho samotnou realizací. Touto změnou by se mělo snížit administrativní zatížení správců, nicméně GDPR nahrazuje oznamovací povinnost dalšími povinnostmi uvedenými níže, které naopak správce pravděpodobně zatíží ještě více. (Burian a Radičová, 2016)

- **Provádět posouzení dopadu na ochranu osobních údajů**

  Prvním mechanismem nahrazující oznamovací povinnost je povinnost provádět posouzení dopadu na ochranu osobních údajů. Tato povinnost by se však měla zaměřit pouze na zpracování, které mohou představovat vysoké riziko z hlediska práv a svobod subjektů údajů. Zda patří zpracování pod vysoce rizikové, či nikoliv, řeší výčtem čl. 35 odst. 3 GDPR. Dozorový orgán pak může zveřejnit podrobnější seznam druhů operací, u kterých posouzení dopadu je a není nutné. Posouzení dopadu bude provedeno posouzením rizik, aplikací testu proporcionality a potvrzením nezbytnosti zpracování. Tuto povinnost, stejně jako nyní povinnost oznamovací, je nutné provést před počátkem zpracování. (Burian a Radičová, 2016)

- **Předběžné konzultace**

  V případě, že zpracování spadá pod povinnost posouzení dopadu na ochranu rizik, je nutné takové případy předem oznámit dozorovému orgánu k předběžné konzultaci. Dozorový orgán pak posoudí, zda je zpracování v souladu s nařízením GDPR. Zatím nevyjasněnou otázkou je pak to, zda posouzení dozorového orgánu bude mít pouze informační charakter, nebo se bude jednat o systém povolení. (Burian a Radičová, 2016)

- **Vést záznamy o zpracování osobních údajů**

  V čl. 30, odst. 1 GDPR se nachází další povinnost, a to: „*Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá*“. Údaje, které je správce povinen zaznamenávat jsou dány výčtem v již zmiňovaném článku. Obdobu této povinnosti pro zpracovatele údajů lze nalézt ve stejném článku v druhém odstavci. Správce, zpracovatel, či je-

jich zástupci jsou pak povinni na vyžádání dozorového orgánu záznamy poskytnout. Obchodnímu závodu odpadá povinnost vést záznamy o zpracování, pokud v obchodním závodě pracuje méně než 250 zaměstnanců a zpracování nelze vyhodnotit jako riziková. (GDPR, 2016)

- **Ohlašovat případy narušení bezpečnosti**

  Povinnost ohlašovat případy narušení bezpečnosti již v současné české legislativě lze nalézt v zákoně č. 468/2011 Sb., o elektronických komunikacích. Jak již z názvu zákonu napovídá, této povinnosti současně platí pouze pro provozovatele elektronických komunikací. GDPR tuto povinnost rozšiřuje na všechny správce. Ti musí nahlásit narušení bezpečnosti osobních údajů dozorovému orgánu do 72 hodin od momentu, kdy se o narušení dozví. Mimo dozorového orgánu musí správce obeznámit s narušením také samotné subjekty, které jsou narušením dotčeny. V rámci GDRP je však také myšleno na drobné pochybení, které nijak zvlášť nemohou narušit práva a svobody jednotlivců, vůči kterým je platná výjimka a ohlašovací povinnost zde není vyžadována. (Burian a Radičová, 2016)

- **Jmenovat pověřence pro ochranu osobních údajů**

  Pověřenec pro ochranu osobních údajů (anglicky Data Protection Officer, zkráceně DPO/pověřenec) je pracovní pozice, kterou v České republice zavádí GDPR. Pověřenec by se měl starat o garanci správného zacházení s osobními údaji v rámci organizace a také obstarávat komunikaci mezi organizací, dozorovým orgánem a veřejností. Zároveň však nesmí v organizaci pracovat na pozici, kde by zpracovával osobní údaje, aby nedošlo ke střetu zájmů. (Škorničková, 2017)

  GDPR v čl. 37 odst. 1 udává následující případy, kdy musí být pověřenec jmenován:

1. *„Zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí.*
2. *Hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů.*
3. *Hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.*“

Pro posouzení, zda je zpracování rozsáhlé je dle Škorničkové (2017) zvážit „*množství zpracovávaných osobních údajů, různorodost zpracovávaných osobních údajů, dobu trvání zpracovávání osobních údajů či geografický rozsah území, z něhož pocházejí zpracovávané osobní údaje*“. Rozsáhlé zpracování tak může splňovat například zpracování osobních údajů v nemocnici, ale zpracování jednotlivým lékařem se již za rozsáhlé nepovažuje.

Celosvětově se odhaduje, že pověřenců bude potřeba kolem 75 000. Nejvíce jich bude v rámci zemí Evropské unie, a to kolem 19 000, 9000 pak ve Spojených státech amerických a přes 7500 v Číně. (Heimes a Pfeifle, 2016)

V jedné organizaci může pozici pověřence vykonávat více osob, ale zároveň jedna osoba může působit jako pověřenec pro skupinu obchodních závodů, pokud bude schopna plnit dostatečně svoje úkoly. (Škorničková, 2017)

Výrazně se oproti současnému stavu legislativy také navýší možné sankce za porušení pravidel stanovenými nařízením GDPR. V současnosti je dle ZoOÚ horní hranice za jeho nejzávažnější porušení nastavena na 10 000 000 CZK. Dle GDPR bude za méně závažné porušení nastavena horní hranice pokuty na 10 000 000 EUR, nebo 2 % z celkového celosvětového obratu za předchozí finanční rok, podle toho, která z hodnot je vyšší. Za závažnější porušení bude pak horní hranice pokuty dvojnásobná, tedy 20 000 000 EUR, nebo 4 % z celkového celosvětového obratu. (Dušek, 2017)

4 Vlastní práce

4.1 Představení společnosti XYZ a.s.

Společnost XYZ a.s. působí v oblasti jazykových služeb prováděných pomocí počítačů. Zákazníci tedy nevyužívají služeb přímo v budovách společnosti, ale jsou jim dodávány pomocí internetové sítě. Společnost působí na trhu téměř 30 let a za dobu svého fungování se značně rozrostla a získala si dobré jméno. Globálně se řadí mezi 10 nejúspěšnějších firem ve svém oboru. Mezi jejich zákazníky patří celosvětově známé společnosti, s jejichž produkty se člověk setkává každý den po celém světě. Mimo Českou republiku již má pobočky ve dvou evropských a čtyřech mimoevropských zemích, což díky různým časovým pásmům zajišťuje téměř celodenní dostupnost poskytovaných služeb. Jazykové služby pak umí dodávat ve více než 150 různých jazycích a mnohým společnostem tak může otevřít příležitost pro vstup na zahraniční trhy. Pro většinu jazyků však používá externí dodavatele z jednotlivých zemí, kteří mohou dodat tu nejlepší kvalitu.

V rámci svojí činnosti se společnost snaží být nejlepší na trhu a dosahuje toho neustálým zaváděním nových technologií. Nespoléhá se však pouze na nástroje dostupné na trhu, ale věnuje se i vytváření vlastních informačně-technologických řešení, které sednou přesně na míru jejich potřebám. Z těchto systémů pak těží nejen společnost XYZ a.s., ale hlavně zákazníci, kteří mohou objednané služby dostat v rychlejším čase a v lepší kvalitě. Pro společnost XYZ a.s. je samozřejmostí osvojení souvisejících ISO norem prokazujících kvalitu služeb.

Zaměstnanci společnosti XYZ a.s. čas od času také přednáší o zajímavých tématech a aktuálním dění na vybraných lingvistických vysokých školách jak v České, tak i Slovenské republice. Přednášky nejsou brány jako forma náborových akcí s cílem najít nové zaměstnance, ale spíše jako představení jak probíhají vyučované metody v praxi. Osobní údaje zde tedy nejsou získávány v žádné formě. Na jedné ze škol se zaměstnanci společnosti XYZ a.s. také přímo podílejí na výuce.

4.2 Obecný úvod k ochraně osobních údajů ve společnosti XYZ a.s.

Společnost XYZ a.s. pro ochranu osobních údajů nemá zavedenou specifickou směrnici. Zaměstnanci, kteří přichází do styku s osobními údaji ostatních, mají však potřebné informace uvedené v pracovní smlouvě a ihned po přijetí jsou náležitě zaškoleni. Dalším zdrojem pro získání informací o zásadách ochrany osobních údajů je ve společnosti XYZ a.s. pracovní řád a směrnice o podpisových pravidlech. Správcem osobních údajů je pak samotná společnost XYZ a.s., což právní řád dovoluje, neboť je společnost XYZ a.s. právním subjektem.

Společnost XYZ a.s. měnila před dvěma roky svoji právní formu včetně změny sídla. To mimo jiné také přineslo změnu identifikačního čísla osoby (IČO). Původní záznam byl v obchodním rejstříku firem vymazán. Při nahlédnutí do veřejného registru zpracování osobních údajů lze však zjistit, že společnost s novou právní formou, sídlem a IČO není u Úřadu pro ochranu osobních údajů zaregistrována. Po vyhledání podle jména společnosti je však společnost XYZ a.s. nalezena, avšak se starým, již neexistujícím IČO, včetně starého sídla společnosti a právní formy. Jednou z povinností správce je udržovat informace o zpracování osobních údajů v aktuálním stavu. Neudržovanou registrací v registru zpracování osobních údajů společnost XYZ a.s. tedy tuto povinnost porušuje. Pro ostatní potřeby této práce bude brána stará registrace jako platná, aby mohly být zhodnoceny další náležitosti registrace společnosti XYZ a.s.

V rámci registrace ve veřejném registru zpracování osobních údajů má společnost XYZ a.s. uveden jako cíl „ochranu majetku správce a třetích osob – plnění účelu smlouvy uzavřené správcem – kontrola plnění pracovních povinností zaměstnanců správce“. Dále je uvedeno, že společnost bude sbírat pouze adresní a identifikační osobní údaje, a to od zákazníků, zaměstnanců, návštěvníků a dodavatelů služeb a zboží. Společnost XYZ a.s. nicméně zpracovává i údaje popisné. Jako příklad lze uvést bankovní spojení, údaje o vzdělání a další. Jako zdrojem osobních údajů pak uvádí přímo subjekty údajů a data z kamerového systému. Společnost XYZ a.s. následně v registraci nemá uvedena žádná další místa, kromě sídla, pro zpracování osobních údajů. V současné době má společnost XYZ a.s. však více poboček, tudíž se zde nachází další nesrovnalost. Ke konci registrace je následně uvedeno, že nebude docházet k předání osobních údajů do jiných států.

4.3 Zpracování osobních údajů před uzavřením pracovního poměru

Prvním případem, kdy se setkává společnost XYZ a.s. s osobními údaji subjektů je výběrové řízení. Díky velikosti společnosti XYZ a.s. se nestává, že by společnost nenabírala nové zaměstnance. Neustále je vypsáno výběrové řízení do několika pozic. Volné pozice společnost XYZ a.s. inzeruje na svých webových stránkách, kde na to má vyčleněnou kariérní sekci. V té se uchazeči mohou kromě informací o otevřených pracovních pozicích dozvědět, jak to ve společnosti funguje, jakou se snaží společnost udržovat kulturu a s jakými činnostmi se mohou zaměstnanci dostat během své práce do styku. Veškeré informace na stránkách, s výjimkou pro pozice, kde není anglický jazyk vyžadován, jsou uvedeny výhradně v angličtině, což efektivně eliminuje uchazeče, kteří angličtinu neovládají. Inzeráty v českém jazyce mají za cíl naopak neodradit uchazeče od projevení zájmu na pozice, kde není anglický jazyk vyžadován. V přihlašovacím formuláři jsou pak uchazeči povinni uvést celé jméno, e-mailovou adresu, telefon a státní příslušnost. Volitelně pak mohou uchazeči přiložit dokumenty jako životopis, motivační dopis a další. Na konci formuláře je uvedeno, že uchazeč jeho

odesláním souhlasí se zpracováním osobních údajů dle zákona č. 101/2000 Sb. o ochraně osobních údajů a dovoluje společnosti XYZ a.s. zpracovávat poskytnuté osobní údaje po dobu, která nepřevýší jeden rok, avšak pouze za účelem výběrového řízení. Tento vyjádřený souhlas se zde však nachází pouze v anglickém jazyce i přesto, že některé pozice jsou uvedeny v jazyce českém. Dle společnosti XYZ a.s. není výjimkou, že uchazeč sám přiloží i vlastní souhlas se zpracováním osobních údajů v rámci dalších dokumentů.

Dále společnost XYZ a.s. inzeruje otevřené pracovní pozice na pracovním portálu Jobs.cz a na portálu Jobote.com, přes který mohou lidé, kromě samotného přihlášení na volnou pozici, doporučovat do vypsaných volných pozic své známé. V případě úspěšného doporučení, které spočívá v přijetí doporučovaného člověka a jeho setrvání po určitou dobu na dosazeném místě, dostane osoba, která zaměstnance doporučila, předem vypsanou odměnu. Společnost XYZ a.s. nabízí za jednotlivé doporučení odměny v řádu desetitisíců korun. Oba zmíněné portály patří pod skupinu LMC s.r.o., která spravuje osobní údaje uchazečů o práci a společnosti XYZ a.s. je poté poskytuje. Na obou serverech se u každé pracovní nabídky nachází zaškrtávací políčko, kterým uchazeč musí vyjádřit souhlas se zpracováním a uchováváním osobních údajů společností XYZ a.s. po dobu tří let a zároveň společností LMC s.r.o. po dobu neurčitou. Zde již je zmíněný souhlas uveden v jazyce inzerátu, tedy v českém jazyce u pozic zadaných v češtině a na stejném principu i u inzerátů v jazyce anglickém. Uchazeč v tomto případě souhlasí s faktem, že společnost XYZ a.s. může s jeho osobními údaji nakládat nejen za účelem výběrového řízení, ale zároveň také může uchazeče zařadit do evidence jakožto potenciálního zaměstnance.

Společnost XYZ a.s. se také aktivně účastní různých pracovních veletrhů, kde představuje svoji společnost a hledá potenciální zaměstnance. Lidé se zde seznámí s konceptem společnosti XYZ a.s. a jsou jim představeny různé pracovní pozice. Většinou je zájemcům pouze předán kontakt na zodpovědnou osobu, se kterou následně řeší podrobnosti o přijímacím řízení, a při samotné komunikaci na pracovním veletrhu tedy k žádnému zpracování osobních dat nedochází. I přesto, že se běžně nestává, že by si zástupce společnosti XYZ a.s. chtěl ponechat zájemcův životopis, má pro jistotu vždy s sebou připraven papírový formulář, kde zájemce může podepsat souhlas se zpracováním osobních údajů.

Ostatní způsoby oslovení zaměstnanců, které dnešní trh nabízí (např. tištěná inzerce, inzerce v rádiu nebo zveřejňování volných pracovních pozic na úřadu práce), společnost nevyužívá. Také se jim zatím ani jednou nestalo, že by někdo bez předchozí komunikace došel fyzicky do budovy společnosti s vytištěným životopisem a tuto skutečnost neočekává díky zaměření jednotlivých pozic, ale i celé společnosti, ani v budoucnu. Veškeré životopisy tedy společnost zpracovává elektronicky. Motivační dopis není k žádným pozicím vyžadován. V případě, že jej uchazeč zašle, je motivační dopis uložen spolu s životopisem, nicméně po přečtení není dál nijak zpracováván.

4.3.1 Průběh výběrového řízení

Jak již bylo zmíněno výše, společnost XYZ a.s. má neustále vypsána alespoň nějaká volná pracovní místa. Průběh výběrového řízení není však pro všechny typy pozic stejný. Doba trvání výběrového řízení se ve společnosti XYZ a.s. pohybuje mezi čtyřmi až dvanácti týdny. Kratší dobu se přijímají řadoví pracovníci, na které nejsou kladeny příliš velké nároky, co se týče znalostí a zkušeností. Delší průběh pak mají výběrová řízení na specificky zaměřené pozice vyžadující hlubokou znalost z daného oboru, řídící a obecně vyšší pozice v rámci společnosti. U těchto pozic personalisté občas přistoupí k telefonickému ověření referencí. Ověřují však pouze fakta, zda daný uchazeč na uváděné pozici opravdu pracoval v období uvedeném v životopise, jakou měl náplň práce a jakých dosáhl výsledků. V rámci ověřování referencí tedy společnost XYZ a.s. nezískává žádné nové osobní údaje.

Výběrové řízení v rámci specificky zaměřených pozic mají tři kola. První kolo je vedeno formou telefonního rozhovoru, kdy po splnění požadavků je uchazeč pozván na ústní pohovor, kde se setká s personalistou. Při příchodu na ústní pohovor je uchazeč vyzván znovu k vyplnění souhlasu se zpracováním osobních údajů. Společnost XYZ a.s. se tak jistí, aby měla uchazečův souhlas fyzicky uložen. V tomto kroku je již uchazeči dán souhlas v českém jazyce. Je-li však uchazečem cizinec, personální oddělení má připraven formulář i v jazyce anglickém. Třetího kola se pak již účastní kromě personalisty i budoucí manažer, pod kterého by daný uchazeč patřil. Na kvalifikačně méně náročné pozice je vynecháno samostatné setkání s personalistou a uchazeč se rovnou setká se svým případným manažerem. V jednotlivých kolech jsou zkoumány uchazečovy dovednosti a znalosti, u vedoucích pozic také soft skills a je posuzováno, zda by do týmu současných zaměstnanců zapadl. Dovednosti a znalosti bývají zkoušeny různými testy relevantními k dané pozici a někdy bývá přistoupeno i k řešení případových studií. Formu assessment centra společnost XYZ a.s. během výběrových řízení nevyužívá a ani její využití v blízké době neplánuje zařadit. Mimo prověřování uchazeče jsou uchazeči v rámci pracovního pohovoru představené činnosti firmy, její zaměření a je mu přiblíženo, co by se od něj na jeho pozici očekávalo. Po proběhnutí pohovoru dává personalista manažerovi doporučení, zda daného člověka přijmout nebo nikoliv, nicméně finální rozhodnutí je v manažerově kompetenci.

Kladný výsledek pohovoru je vždy oznámen telefonicky a následně je vybranému uchazeči e-mailem zaslána oficiální pracovní nabídka (job offer). Tato nabídka obsahuje uchazečovo jméno, mzdový návrh, zda je nabídka smlouvy na dobu neurčitou a v případě smlouvy na dobu určitou je zároveň uvedena doba jejího trvání. Dále jsou uvedeny další specifické údaje jako nabízené benefity nebo informace o práci z domova.

Negativní výsledky pohovorů jsou uchazečům oznámeny e-mailem v případě vyřazení uchazeče během prvních výběrových kol. Pokud uchazeč přes první kola prošel a následně nebyl vybrán v kolech dalších, tak je již vyrozumění podáno telefonicky. Společnost XYZ a.s. neudržuje žádnou databázi potenciál-

ních zaměstnanců, a tak veškeré osobní údaje neúspěšných uchazečů společnost XYZ a.s. po ukončení výběrového řízení přesouvá ihned ke skartaci, jak mají uvedeno ve skartačním řádu, respektive se mažou z počítačových úložišť. Společnost XYZ a.s. tak neporušuje svůj závazek, který s uchazečem uzavřela podepsáním souhlasu se zpracováním osobních údajů za účelem výběrového řízení. Nutno podotknout, že v případě, kdy uchazeč reagoval skrze jeden z webových portálů patřící pod společnost LMC s.r.o., má společnost XYZ a.s. právo uchovávat uchazečovy osobní údaje ještě po dobu tří následujících let v rámci zařazení uchazeče do skupiny potenciálních zaměstnanců.

Během průběhu výběrového řízení se dokumenty jako životopis, či kopie e-mailové komunikace, dostávají nejdříve k personalistovi, který je následně umístí do intranetové sítě a přidá přístupová práva relevantním manažerům. K osobním údajům uchazečů se tak dostanou opravdu pouze nezbytní zaměstnanci, kteří se na přijímacím řízení podílí.

4.4 Zpracování osobních údajů v době trvání pracovního poměru

Úspěšný uchazeč musí před finálním podepsáním smlouvy podstoupit ještě některé další povinnosti. První oficiální komunikací mezi společností XYZ a.s. a budoucím novým zaměstnancem je zaslání pracovní nabídky (job offeru), podle kterého se pak rozhoduje o termínu nástupu. Datum nástupu je následně zvoleno v období pěti až dvaceti dnů po přijmutí nabídky. V případě, že uchazeč tuto nabídku přijme, jsou mu zaslány instrukce, co musí před nástupem vše vyřídit/vyplnit. Mezi tyto požadavky patří vyplnění osobního dotazníku, doložení dosaženého vzdělání, případně příslušných certifikací, je-li to nutné, dále potvrzení o trestní bezúhonnosti a potvrzení o zdravotní způsobilosti k výkonu práce. Potvrzení o zdravotní způsobilosti si může úspěšný uchazeč vyřídit u svého stálého doktora, nicméně společnost XYZ a.s. mu nabídne i doktora závodního. Společnost XYZ a.s. spadá do první kategorie (nepravděpodobný nepříznivý vliv na zdraví) dle zákona o ochraně veřejného zdraví, tudíž touto prohlídkou projde téměř každý.

Mimo povinnosti uchazeče začnou probíhat mnohé procesy i na pracovišti zaměstnavatele. Začíná se připravovat pracovní místo, vybírá a nastavuje se veškerý hardware, který bude nový zaměstnanec potřebovat, nastavují se mu příslušná přístupová práva jak v rámci počítačového rozhraní, tak i na přístupy do budov a zařizuje se mu přístupová čipová karta.

4.4.1 Podepsání pracovní smlouvy a smlouvy o mzdě

K podepsání smlouvy se musí vybraný uchazeč již dostavit se všemi vyřízenými dokumenty, které jsou uvedené v předchozí kapitole. Tuto dokumentaci následně odevzdává personalistovi. Po kontrole dokumentů je vybranému uchazeči dán k prostudování pracovní a mzdový řád. Poté již může uchazeč přistoupit k podepsání smluv. Smlouvy se podepisují dvě. První je smlouva pracovní, kde

jsou uvedeny povinné náležitosti jako druh práce, místo výkonu práce a den nástupu a následně další podmínky za jakých se smlouva uzavírá. Zároveň se v rámci pracovní smlouvy také uchazeč zavazuje dodržovat dříve uvedené řády. V rámci těchto řádů jsou reference na další podnikové směrnice, nicméně ty může uchazeč prostudovat a potvrdit jejich prostudování v interním informačním systému kdykoliv poté. Veškeré řády a směrnice vede společnost XYZ a.s. v českém i anglickém jazyce.

Co však v rámci pracovní smlouvy nelze nalézt je explicitně vyjádřená výše mzdy, nicméně pouze odkaz na smlouvu o mzdě. Výše mzdy však není povinnou náležitostí pracovní smlouvy, tudíž společnost jedná dle zákona.

Smlouva o mzdě je se zaměstnancem uzavírána ve stejnou dobu jako pracovní smlouva. Společnost XYZ a.s. se rozhodla pro tyto oddělené smlouvy z důvodu ulehčení administrace. Mzda zaměstnanců se může měnit i několikrát během roku a díky zmíněnému nastavení je nutné aktualizovat pouze smlouvu o mzdě a zaměstnanci tak nemusí kontrolovat znovu celou pracovní smlouvu. Mzdu mají stálí zaměstnanci uvedenou v roční sazbě. Brigádníci mají sazbu uvedenou hodinově z důvodu krátkodobé a často nepravidelné docházky.

Společnost XYZ a.s. využívá širokou škálu dostupných smluv a jejich jednotlivých variant. Pro své stálé zaměstnance nabízí smlouvy jak na neurčito, tak i na dobu určitou. Co se týče brigádníků, využívá společnost XYZ a.s. nejdříve dohody o provedení práce a následně po vyčerpání ročního hodinového limitu každého zaměstnance dohody o pracovní činnosti. V rámci brigádnických pracovních dohod je mzda sjednána přímo v dané dohodě a oddělení mzdy do smlouvy o mzdě zde společnost XYZ a.s. nevyužívá.

Smlouvy jsou vždy vyhotoveny ve dvou provedeních. Jedno si nechává společnost XYZ a.s. a druhé provedení dostane nový zaměstnanec. V případě, že novým zaměstnancem je cizinec, dostává smlouvu ve dvou variantách, a to v českém a anglickém jazyce. V současné době chystá společnost XYZ a.s. novou variantu těchto smluv, kdy bude smlouva pouze jedna dvojjazyčná, aby zaměstnanci ze zahraničí neměli problém při jednání na úřadech.

Po podepsání smlouvy jsou zaměstnanci ve stejný den proškoleni o bezpečnosti a ochraně zdraví při práci a požární ochraně.

4.4.2 Osobní dotazník zaměstnance

Osobní dotazník si společnost XYZ a.s. sestavila sama dle vlastních potřeb. Budoucímu zaměstnanci je odeslán k vyplnění po přijetí pracovní nabídky a je povinen ho vyplnit a odevzdat personalistovi před podepsáním pracovní smlouvy. Součástí osobního dotazníku jsou pouze identifikační a adresní údaje. Společnost XYZ a.s. v osobním dotazníku nepožaduje po zaměstnanci žádné citlivé údaje, které je možno nalézt explicitně vypsány v § 4 písm. b) ZoOÚ.

Osobní dotazník je připraven i v anglickém jazyce pro zaměstnance přicházející ze zahraničí. Pokud navíc pochází ze státu mimo Evropskou unii, Evropského hospodářského prostoru nebo Švýcarska, musí navíc vyplnit, zda souhlasí s přihlášením do všeobecné zdravotní pojišťovny a číslo pasu. Číslo pasu, re-

spektive jiného dokladu prokazujícího totožnost je vyžadováno pro vedení mzdových listů dle § 38j odst. 2 písm. b) zákona č. 586/1992 Sb. o daních z příjmu.

Zaměstnanec také odevzdáním stvrzuje, že tyto údaje, můžou být použity pro účetní, mzdovou a personální agendu společnosti XYZ a.s. po nezbytně nutnou dobu.

4.4.3 Osobní spis zaměstnance

Společnost XYZ a.s. vede osobní spis zaměstnance jak v papírové, tak i elektronické podobě. Ne všechny dokumenty jsou však uchovávané v obou variantách. Platí, že v papírové formě jsou uchovávány veškeré dokumenty. V elektronické podobě pak uchovává společnost XYZ a.s. pouze dokumenty, které v elektronické formě byly vytvořeny. Nestává se tedy, že by se dokumenty získané od zaměstnance digitalizovaly a následně ukládaly v počítači. Výjimkou je pouze osobní dotazník, ze kterého se musí ručně přenést data do interního informačního systému.

V papírovém osobním spisu jsou shromažďovány veškeré dokumenty týkající se daného zaměstnance. Patří sem pracovní smlouva, smlouva o mzdě a případně veškeré jejich dodatky, dodatky o práci z domu a odpovědnosti za majetek, doložení nejvyššího dosaženého vzdělání, osobní dotazník, potvrzení o trestní bezúhonnosti, potvrzení o absolvování školení o bezpečnosti a ochraně zdraví při práci, požární ochraně a dalších školení. Obecně tedy všechny dokumenty, co vzniknou se jménem zaměstnance. V osobním spisu zaměstnance je také uložen výsledek vstupní lékařské prohlídky, tedy zda je zaměstnanec schopen k výkonu dané práce.

Janečková a Bartík (2016) upozorňují, že pouhé potvrzení o zdravotní způsobilosti není bráno jako citlivý údaj o zdravotním stavu dle § 4 písm. b) ZoOÚ. Správce tedy v případě uchovávání těchto informací není povinen zařadit do oznámení Úřadu, že zpracovává citlivé údaje.

Společnost XYZ a.s. nepořizuje, a tím pádem ani nezařazuje, do osobního spisu zaměstnance kopii občanského průkazu. Občanský průkaz vyžaduje pouze k nahlédnutí pro kontrolu správnosti údajů v osobním dotazníku. Jedinou výjimkou jsou zaměstnanci ze třetích zemí, u kterých společnost XYZ a.s. ze zákona musí vést záznam o číslu občanského průkazu nebo pasu. V takovém případě je do osobního spisu pořízena kopie zvoleného dokladu.

Změnu osobních údajů je zaměstnanec povinen oznámit zaměstnavateli. Dle různých dokumentů je však pokaždé jiná lhůta na provedení této změny. V pracovním řádu se zavazuje zaměstnanec ke lhůtě osmi dnů ode dne, kdy změna nastala. V osobním dotazníku je pak uvedena lhůta kratší, pouze třídenní. Kromě těchto bodů pak již zaměstnancovi není povinné hlášení aktualizací jeho osobních údajů připomínáno nikde.

Listinná podoba osobních spisů zaměstnanců je uložena na personálním oddělení, kam mají přidělena vstupová práva pouze zaměstnanci personálního oddělení. Stejná situace je i na oddělení finančním. Dokumenty jsou následně

uloženy v plechových skříních na zámek. I pokud by se tedy stalo, že se někdo dostane do místnosti, kde jsou dokumenty v listinné podobě uloženy, tak se k těmto dokumentům nedostane. Ochrana listinné podoby dokumentů je tak dostatečná.

4.4.4 Čipová karta

Čipovou kartu dostává každý zaměstnanec při příležitosti dne nástupu do práce, včetně brigádníků. Kromě nich pak dostávají čipovou kartu dočasně i návštěvníci, což mohou být například i uchazeči o zaměstnání přicházející na pohovor. Zaměstnanecké čipové karty jsou označeny jménem, příjmením a fotkou zaměstnance. Ostatní mají pak kartičku s viditelným označením „dočasný“, nebo „host“. Název firmy není z bezpečnostních důvodů při ztrátě karty uveden ani na jedné z variant. Tuto čipovou kartu musí mít dotyčný při sobě po celou dobu svého pobytu v dané budově a na příslušných místech se s ní prokázat. Její ztrátu je pak povinen nahlásit zaměstnavateli do 24 hodin.

Čipové karty primárně slouží k umožnění vstupu do budovy, jednotlivých pater a případně i místností. Na každé čipové kartě si její uživatel nastaví pin kód. Tento kód však není vyžadován vždy. Využíván je zejména při vstupech do budovy mimo běžnou pracovní dobu, vstupech do jiné budovy, než ve které zaměstnanec normálně pracuje, nebo do určitých místností s vyšší úrovní zabezpečení. Ke každé kartě je možné nastavit vstupní práva jednotlivě.

Dalším účelem čipové karty je kontrola docházky. Každý zaměstnanec má povinnost při každém příchodu a odchodu z budovy tuto činnost zaregistrovat pomocí čipové karty. Údaje z čipové karty jsou pak základem pro vyplnění měsíčního výkazu práce.

Čipová karta je odevzdávána společnosti v poslední den zaměstnancova pracovního poměru, případně při odchodu návštěvy.

4.4.5 Fotografie

Společnost XYZ a.s. pořizuje při podepisování smluv jednu portrétovou fotografii nového zaměstnance. Ten pak v rámci osobního dotazníku stvrzuje, že fotografie může být použita pro interní potřeby. Fotka se následně zobrazuje v interním informačním systému, zaměstnanec si ji může zvolit jako fotku u e-mailové pošty a také se vyskytuje na čipové kartě zaměstnance.

Další fotografie bývají nepravidelně pořizovány na společenských aktivitách pořádaných společností XYZ a.s. Těchto aktivit zaměstnanci nejsou povinni se zúčastňovat a předem jim je oznámeno, že se budou fotografie pořizovat. Ty jsou většinou uveřejněny v rámci podnikové sítě. Samozřejmostí je pak vynechání nelichotivých fotek a každý zaměstnanec má v případě nelibosti právo zažádat o smazání jakékoliv fotografie, které je součástí. V případě, kdy by se měla jakákoliv fotografie zveřejňovat mimo firemní síť, jmenovitě například na webové stránky společnosti XYZ a.s., nebo na její Facebookový profil, je každý z účastníků dané fotografie kontaktován, zda s uveřejněním souhlasí.

4.4.6 Informační systémy

V oblasti personálních a mzdových prací používá společnost XYZ a.s. zakoupené informační systémy. První informace o novém zaměstnanci jsou do něj ručně přepsány z vyplněného osobního dotazníku. Poté se postupně plní relevantními informacemi k výplatám, číslem zaměstnancova bankovního účtu, informacemi o daňových srážkách a mnohými dalšími. V rámci České republiky společnost XYZ a.s. používá samostatný informační systém, který je pravidelně aktualizován v souladu s českou legislativou. Z toho informačního systému se také vypočítávají a odesílají mzdy zaměstnancům. Ve všech pobočkách společnosti XYZ a.s. je pak používán jeden univerzální informační systém, který komunikuje se mzdovými systémy v jednotlivých zemích.

Do personálního informačního systému používaného pouze v rámci České republiky mají přístup pouze zaměstnanci personálního a finančního oddělení. Tento systém není webový, a tak do něj lze přistupovat pouze skrze softwarového klienta. Tím je tento chráněn proti jakýmkoliv útokům z venčí a osobní data zaměstnanců jsou tak bezpečně chráněna. Do mezinárodního personálního informačního systému pak mají přístup všichni zaměstnanci a mohou zde prohlížet informace o své osobě. Naleznou zde svoje osobní údaje, informace o nástupu, o mzdovém ohodnocení a také informace o veškerých školení a certifikacích, které byly získány v rámci společnosti XYZ a.s. Tento profil zaměstnance si mohou prohlédnout také jeho nadřízení, aby viděli, jak se například zaměstnanci v jeho týmu snaží vzdělávat, případně jak jsou ohodnoceni.

Zabezpečení obecně jak pro jednotlivé informační systémy, tak i pro samotné počítače je řešeno pomocí hesel. Každý zaměstnanec si zvolí svoje a nesmí ho nikomu sdělovat. Každé dva měsíce je pak zaměstnanec vyzván informačním systémem, aby si heslo v rámci bezpečnosti změnil. Pokud změnu neprovede, je mu účet zablokován a musí si ho nechat obnovit IT oddělením. V pracovním řádu je pak uvedeno, že při každém opuštění pracovního místa musí zaměstnanec svůj počítač uzamknout, aby zamezil přístupu jiných zaměstnanců k jeho informacím. Mimo zmíněné opatření proti zásahům neoprávněných má osob společnost XYZ a.s. veškeré počítače hlídány aktualizovaným antivirovým programem.

4.4.7 Předávání osobních údajů do zahraničí

Společnost XYZ a.s. má svoje pobočky jak na území Evropské unie, tak i v ostatních mimoevropských zemích. Je tedy vhodné prozkoumat i oblast předávání osobních údajů do zahraničí.

Předávání osobních údajů do zahraničí se věnuje § 27 ZoOÚ. Dle tohoto zákona je nutné rozlišovat dvě hlavní skupiny pravidel. Do první skupiny se řadí členské země Evropské unie, kde platí volný pohyb osobních údajů. V takovém případě tedy mohou společnosti předávat osobní údaje do ostatních států bez dalšího omezení a nemusí tuto skutečnost ani ohlašovat Úřadu. Do této skupiny lze také zařadit země, které splňují zvláštní podmínku dle § 27 odst. 2 ZoOÚ,

tedy pokud zákaz omezení volného pohybu vyplývá z mezinárodní smlouvy, jakou může být například Úmluva č. 108.

Do druhé skupiny lze pak zařadit veškeré ostatní země. Pokud chce společnost předávat osobní údaje do země z této skupiny, musí dle § 27 odst. 4 ZoOÚ požádat Úřad o povolení k předání před jeho samotným počátkem. Úřad následně stanoví, zda vůbec a případně po jakou dobu může předávání probíhat. Předání pak musí splňovat některou z podmínek uvedených v § 27 odst. 3 ZoOÚ, kde nejčastěji bývá využívána podmínka z písm. a), která říká, že se předání údajů do třetí země děje se souhlasem subjektu údajů. (Bartík, 2013)

Společnost XYZ a.s. v rámci své registrace výslovně uvedeno, že nebude docházet k předání osobních údajů do jiných států. Jak již bylo uvedeno, společnost XYZ a.s. má zaměstnance v různých koutech světa. Jak v Evropě, tak i mimo ni, zejména pak i v třetích zemích, které nejsou zahrnuty ve výjimce dle § 27 odst. 2 ZoOÚ. Je běžnou praxí, že například zaměstnanec v České republice má manažera v mimoevropské zemi. V rámci výkonu práce má manažer v informačním systému účelný přístup k informacím o jeho podřízených, v tomto případě tedy o zaměstnanci v České republice. V takovém případě se jedná o předávání osobních údajů do zahraničí, které se řídí podle § 27 ZoOÚ. Společnost XYZ a.s. se tedy v případě předání osobních údajů do třetích zemí nepodléhající podmínce uvedené v § 27 odst. 2 ZoOÚ může dostat do rozporu se zákonem o ochraně osobních údajů.

4.5 Monitorování zaměstnanců

4.5.1 Kamerový systém

Společnost XYZ a.s. má ve svých budovách hodně cenného vybavení. Mezi takové patří hlavně stolní počítače a jejich příslušenství, jelikož téměř každý zaměstnanec má přidělen jeden až dva počítače, většinou včetně dvou monitorů. Z tohoto důvodu společnost XYZ a.s. využívá na svých pobočkách kamerový systém se záznamem. Účel kamerového systému je stanoven jako ochrana majetku správce a třetích osob. Společnost XYZ a.s. tak využívá výjimku uvedenou v § 316 odst. 2 ZPr. Jednotlivé kamery jsou umístěné u vstupů do budov, vstupů do jednotlivých pater a případně u vstupů do prostor se zvláštním účelem. Vstupy do jednotlivých pater jsou kamerami sledovány z obou směrů, tedy ze schodiště do kancelářských prostor i naopak. I přesto, že se kamery nachází v kancelářských prostorech, jsou tyto kamery směřovány pouze na vstupové dveře. Nemůže se tedy stát, že by bylo narušeno soukromí zaměstnanců například kamerovým sledováním jejich monitorů, či záběry šaten. Díky tomu může společnost XYZ a.s. také aplikovat výjimku uvedenou v § 5 odst. 2 písm. e) ZoOÚ, ze které plyne, že společnost XYZ a.s. nemusí vyžadovat souhlas subjektu údajů s pořizováním kamerového záznamu, protože tato činnost správce je nezbytná pro ochranu jeho práv a není v rozporu s právem subjektu údajů na ochranu jeho osobního a soukromého života.

Kamerový systém má společnost XYZ a.s. korektně nahlášen jako zdroj osobních údajů v rámci registrace ve veřejném registru zpracování osobních údajů, včetně jeho cíle. Kamerový systém však společnost XYZ a.s. nemá na všech budovách správně označen. V první navštívené budově bylo vše označeno bez problémů. V oblasti ve výšce očí se nacházela nálepka s piktogramem o provozování kamerového systému a informacemi o správci údajů v českém jazyce, včetně kontaktu na něj. I přesto, že to nežádá zákon, bylo by vhodné informace uvést i v jazyce anglickém, jelikož ve společnosti XYZ a.s. pracují, případně ji i často navštěvují, lidé ze zahraničí. V druhé budově byly sice prostory označeny tabulkou s piktogramem o provozování kamerového systému, nicméně zde zcela chyběla jakákoliv další informace o správci údajů. Tabulka s piktogramem navíc byla umístěna skoro metr nad oblast očí a leckdo by tak toto označení mohl přehlédnout.

Diskutabilní je i doba uchovávání záznamů z kamerového systému. Ta je nyní ve společnosti XYZ a.s. nastavena na dobu 30 dnů. Dle § 5 odst. 1 písm. d) ZoOÚ je správce povinen uchovávat pouze po dobu, která je nezbytná pro naplnění účelu jejich zpracování. Tato lhůta není nikde striktně uvedena, nicméně Úřad pro ochranu osobních údajů ve své tiskové zprávě z roku 2006 uvedl, že by tato lhůta neměla překročit několik dní. Oproti tomuto vyjádření se lhůta 30 dnů zdá spíše přehnaná a svádí k neoprávněnému využití záznamu.

Záznamy z kamer se však běžně nekontrolují a je do nich nahlíženo pouze v případě vyšetřování bezpečnostního incidentu. K záznamům má přístup pouze velmi omezená skupina lidí. Záznamy jsou uchovávány v zabezpečené serverovně, kam mají zaměstnanci přístup omezen pomocí nastavení čipové karty. V oblasti bezpečnosti jsou tedy kamerové záznamy pořizované společností XYZ a.s. v pořádku.

4.5.2 Monitorování e-mailové pošty a přístupů na internet

Společnost XYZ a.s. umožňuje svým zaměstnancům používat jak e-mailovou poštu, tak i přístup k internetu pro své soukromé potřeby, tedy i mimo plnění pracovních úkolů. Tato soukromá činnost musí být využívána v rozumné míře a nesmí být žádným způsobem ohroženo plnění požadovaného pracovního výkonu zaměstnance. Zaměstnanci jsou o těchto pravidlech informováni v rámci pracovního řádu.

Každá z forem má však svoje další omezení, které zaměstnanci musí respektovat. E-mailovou poštu sice zaměstnanec může používat pro soukromé účely, nicméně ji nesmí využívat k vykonávání vlastní výdělečné činnosti, či rozesílání hromadné nevyžádané pošty. Internet pak zaměstnanec nesmí používat zejména ke hraní her, navštěvování stránek ke stahování softwaru a jakýchkoliv jiných dat, pokud to není nezbytné k plnění pracovních úkolů, a obecně dalších stránek, které jsou v rozporu s etickými pravidly. Na některé specifické stránky jsou přístupy blokovány přímo společností XYZ a.s., takže se k nim zaměstnanec nemůže vůbec připojit, nicméně ostatní využívání by si měl zaměstnanec hlídat sám.

Společnost XYZ a.s. svým zaměstnancům věří a žádnou průběžnou či namátkovou kontrolu využívání přístupu na internet a e-mailové pošty nevyužívá. I přesto, že zákon zaměstnavateli dovoluje nahlížet do e-mailové pošty zaměstnance kvůli jeho dlouhodobé či neočekávané absenci za účelem snížení rizika nevyřízených pracovních záležitostí, společnost XYZ a.s. tuto možnost nevyužívá. Zaměstnanci mají ke své e-mailové poště umožněn vzdálený přístup, takže nutnou e-mailovou korespondenci mohou vyřizovat kdekoliv, kde se mohou připojit k internetu. Zaměstnanec si v takovém případě většinou nastaví automatickou odpověď ohledně jeho nepřítomnosti a případně zvolí přesměrování jeho e-mailové pošty na některého z kolegů. V případě vážnějšího stavu zaměstnance, kdy není v jeho možnostech, aby v jeho absenci podnikl zmiňované kroky pro vyřizování e-mailové korespondence, společnost zašle informativní e-mailovou zprávu relevantním pracovním skupinám, se kterými daný zaměstnanec přichází do styku, o jeho absenci s instrukcemi na koho se obracet v jeho nepřítomnosti.

4.5.3 Monitorování služebních telefonů a automobilů

Téměř každý zaměstnanec ve společnosti XYZ a.s. má na svém pracovním stole pevnou linku, někteří zaměstnanci, hlavně na vyšších pozicích, pak mají i služební mobilní telefon. Společnost XYZ a.s. umožňuje svým zaměstnancům využívat tyto telefony i pro soukromé účely, nicméně soukromé hovory si každý zaměstnanec musí uhradit sám. U obou variant telefonů má každý zaměstnanec pro případy soukromých hovorů přidělený kód, který musí zadat před vytáčením čísla, aby soukromý hovor oddělil od hovorů pracovních. Nahromaděná částka za soukromé hovory se pak každý měsíc strhne zaměstnancovi ze mzdy.

Společnost XYZ a.s. s tímto systémem fungování doposud neměla problém. Zaměstnanci dle jejího vyjádření telefony skoro nevyužívají. Většina komunikace se přesunula na internetovou telefonii využívající Skype, Jabber a další podobné programy. I z těchto důvodů zatím společnost XYZ a.s. nepřistoupila k provádění kontrol, ať už pravidelných či namátkových, zda zaměstnanci nezneužívají pracovních hovorů pro hovory soukromé. Právo na to ovšem má. V rámci pracovního řádu má společnost XYZ a.s. stanoveno, že pokud dojde k podezření využívání pracovních hovorů k hovorům soukromým, je zaměstnanec povinen identifikovat volané číslo a doložit účel hovoru. Jediným používaným omezením je blokování prémiových telefonních hovorů a SMS zpráv, se kterými by zaměstnanec v rámci pracovního poměru neměl vůbec přijít do styku. Toto omezení je nastaveno přímo u operátora a zaměstnanec si ho nemůže měnit.

Přístup společnosti XYZ a.s. k monitorování služebních telefonů není v rozporu s žádným zákonem.

Žádný ze zaměstnanců společnosti XYZ a.s. nemá přidělen služební automobil, čímž je tato problematika pro společnost XYZ a.s. irelevantní a nemají pro ni ustanovená žádná specifická pravidla.

4.6 Zpracovávání osobních údajů po ukončení pracovního poměru

Při ukončení pracovního poměru je zaměstnanci vydáno potvrzení o zaměstnání, případně posudek o pracovní činnosti, pokud si o to zaměstnanec zažádá. V oblasti dokumentace se společnost XYZ a.s. řídí ustanoveným skartačním řádem. Pracovní smlouvy, mzdové listy a účetní záznamy pro účely důchodového pojištění před konečnou skartací archivuje dle zákona po dobu 30 let a záznamy o mzdách a odpracovaných hodinách 5 let. Veškerý obsah osobní složky, kterým ukončením pracovního poměru pomine účel zpracování, jsou buď předány danému subjektu údajů, nebo jsou ihned určeny ke skartaci. Patří sem zejména životopis, motivační dopis a kopie osvědčení o dosaženém vzdělání. V případě, že zaměstnanec během svého pracovního poměru získal nějaké certifikace, jsou mu vydány v den ukončení pracovního poměru. Společnost XYZ a.s. nicméně dodává, že naprostá většina jimi poskytovaných školení je pouze interní a ostatní certifikace si zařizují zaměstnanci ve své režii, takže je společnost XYZ a.s. u sebe fyzicky nemá.

V případě, že zaměstnanec v rámci svého pracovního poměru uzavřel dohodu o odpovědnosti, provádí se ještě navíc inventura spojená s jeho výkony.

5 Návrhy a doporučení

5.1 Oprava registrace v registru zpracování osobních údajů

Společnost XYZ a.s. měnila před pár lety svoji právní formu a sídlo, která vyústila také ve změnu identifikačního čísla osoby (IČO). Prvním, ale zároveň vcelku závažným, rozporem oproti platné legislativě, je neplatná registrace v registru zpracování osobních údajů. V rámci registrace je správce povinen udržovat aktuální informace o jím prováděném zpracování osobních údajů. Společnost XYZ a.s. však od počátku své registrace změnu neprovedla. Neprovedla ji ani po změně právní formy. Společnost XYZ a.s. s novým IČO tak není v současné době vůbec zaregistrována, čímž se prohřešuje nesplněním oznamovací povinnosti podle § 16 ZoOÚ. Tento delikt lze nalézt v prvním odstavci § 45 písm. i) ZoOÚ a společnosti XYZ a.s. za něj hrozí pokuta až do výše 5 000 000 Kč, jak je uvedeno v § 45 odst. 3 ZoOÚ.

Pokud však porovnáme nynější stav zpracování ve společnosti XYZ a.s. s původní registrací, není opomenutí nové registrace jediným prohřeškem. Společnost XYZ a.s. má svoje podnikání rozprostřeno do několika budov, ve kterých probíhá pořizování a zpracování osobních údajů, nicméně v rámci registrace nemá uvedena žádná další místa zpracování, než sídlo společnosti. Oznámení míst zpracování osobních údajů je vyžadováno v § 16 odst. 2 písm. f) ZoOÚ. Porušení této povinnosti lze zařadit do stejné kategorie jako delikt uvedený výše, tedy pokutovatelný s horní hranicí 5 000 000 Kč.

Dalším rozporem je pak oblast předávání osobních údajů do jiných států. V registraci má společnost výslovně uvedeno, že k předávání osobních údajů do jiných států nebude docházet, nicméně v praxi jsou data postupována dalším lidem v zahraničí, a to i včetně států, které nespadají do pod výjimku dle § 27 odst. 2 ZoOÚ. Děje se tak v případech, kdy zaměstnanci mají nadřízeného z jiného státu. V takovém případě má nadřízený přístup k osobním údajům svého podřízeného. Nenahlášením této skutečnosti se společnost XYZ a.s. prohřešuje proti § 16 odst. 2 písm. h) ZoOÚ. V rámci pokutování se tento delikt zařazuje do skupiny s horní hranicí pokuty 5 000 000 Kč.

Poslední nesrovnalostí je pak neuvedení zpracování popisných údajů, které společnost XYZ a.s. ve skutečnosti zpracovává. Povinnost uvést kategorie osobních údajů lze nalézt v § 16 odst. 2 písm. c) ZoOÚ. Tento delikt je možné, stejně jako předchozí delikty, pokutovat za porušení § 45 odst. 1 písm. i) ZoOÚ a spadá tak do kategorie deliktů s horní hranicí pokuty 5 000 000 Kč.

Společnost XYZ a.s. by tak měla celou registraci v registru zpracovávání osobních údajů provést znovu. Novou registraci je možno provést přes webové rozhraní Úřadu pro ochranu osobních údajů. Společnost XYZ a.s. by si oproti předešlé registraci měla dát pozor zejména na nové IČO, změnu sídla, zahrnutí veškerých dalších míst zpracování osobních údajů, uvedení všech typů zpracovávaných kategorií osobních údajů, a také na část předání osobních údajů subjektů do zahraničí.

Samotným vyplněním registrace však společnost nesplní povinnost požádat Úřad o povolení k předávání osobních údajů do jiných zemí, která je uvedena v § 27 odst. 4 ZoOÚ. Společnost XYZ a.s. tak musí Úřadu zaslat samostatnou žádost o vydání povolení k předání osobních údajů do jiných zemí. Tato žádost by měla obsahovat země, kam budou osobní údaje předávány, kategorie předávaných osobních údajů, jejich zdroj, účel a dobu zpracování. Úřad následně rozhodne, zda předání povolí, a také na jakou dobu.

Společnost XYZ a.s. by se také měla vypořádat se starou registrací. Při ukončení činnosti zpracování osobních údajů správcem, v tomto případě kvůli přechodu na novou právní formu společnosti, tedy nového správce, má správce povinnost dle § 19 ZoOÚ neprodleně uvědomit Úřad včetně informací, jak bude naloženo se zpracovanými osobními údaji. Toto oznámení může správce provést prostřednictvím e-mailu s elektronickým podpisem, klasickým dopisem, nebo zasláním zprávy pomocí datové schránky.

Veškeré uvedené úkoly by měl zpracovat právník společnosti XYZ a.s., jehož mzda přepočtená na hodinu vychází přibližně na 240 Kč. Mzdu sice dostává fixní dle smlouvy o mzdě, nicméně tuto činnost bude muset vykonávat na úkor jiné, a proto je vhodné vyčíslit, kolik tento návrh bude firmu stát. Seznámení se se současným stavem zpracování osobních údajů ve společnosti XYZ a.s. a s nutnými částmi platné právní úpravy zákona 101/2000 Sb. o ochraně osobních údajů by měl právník stihnout během pěti hodin. Nová registrace by mu pak neměla zabrat více než dvě hodiny, jelikož ji lze provést online na webových stránkách Úřadu, kde je potřeba pouze vyplnit k tomu určený formulář. Jelikož už bude mít právník veškeré podklady připraveny, nemělo by mu pak trvat více než hodinu vytvoření žádosti o povolení k předávání osobních údajů do jiných zemí, jejíž vzor lze nalézt na webových stránkách Úřadu. Poslední činností, která by měla uvést oznámení do souladu s platnou právní úpravou je oznámení ukončení zpracování osobních údajů, které by po předchozích krocích měl právník stihnout během dvou hodin. Za registraci, její zrušení, či další činnosti související s Úřadem si Úřad neúčtuje žádné poplatky. Jako další náklad se zde vybízí změna informačních tabulek oznamujících monitorování objektu pomocí kamerového systému, jelikož je na ní v současné době uveden správce údajů dle původní registrace. Tento náklad však bude zařazen v jednom z dalších návrhů. Výsledným nákladem je tedy 10 hodin práce právníka, které jsou oceněny na 2 400 Kč, což je oproti horní výši potenciální pokuty 5 000 000 Kč zanedbatelná částka.

5.2 Správné označení budov o monitorování subjektů údajů kamerovým systémem

Každý správce osobních údajů, který provozuje ve svých budovách kamerový systém, je povinen střežené prostory zřetelně označit. Na jedné z budov společnosti XYZ a.s. je kamerový systém označen zcela dle předpisů. Před vstupem do samotné budovy se ve výšce očí nalézá tabulka s piktogramem kamery a textem

upozorňujícím, že je objekt střežen kamerovým systémem. Vedle této tabulky je pak uveden správce s kontaktem, kam je možné se obrátit pro podrobnější informace o kamerovém systému.

Na druhé budově společnosti XYZ a.s. je však tabulka s piktogramem kamery umístěna výrazně nad linii očí, což ji činí lehce přehlédnutelnou. Dále zde pak nejsou uvedeny žádné další údaje o správci, či kontaktu na něj. Tyto informace jsou vyžadovány dle metodiky pro provozování kamerových systémů vydané Úřadem (2012). Společnost XYZ a.s. by tak měla minimálně na této budově přistoupit k nápravě. Aby však bylo označení jednotné na obou budovách, bude lepší vytvořit nové označení pro obě budovy, které bude odpovídat požadavkům metodiky Úřadu.

Jelikož má jedna z budov dva samostatné vchody, ze kterých je možné se do budovy dostat, bude potřeba veškeré značení minimálně ve třech provedeních. Tabulky k označení lze pořídit za téměř zanedbatelnou částku, a proto bude pro společnost XYZ a.s. praktičtější, když objedná nějaké do zásoby. Bude tedy uvažováno jednou tak velké množství, než je minimální, tedy šest tabulek s označením kamerového systému a 6 tabulek s informacemi o správci. Jelikož objekty společnosti XYZ a.s. navštěvují i osoby ze zemí mimo Českou republiku, je dle metodiky Úřadu vhodné uvést informace o správci také v cizím jazyce. Z důvodu, že v rámci celé společnosti XYZ a.s. je používán všemi anglický jazyk, bude i informování o správci údajů uvedena v angličtině. Překlad si firma zařídí ve vlastní režii. V následující tabulce je možno vidět předpokládanou kalkulaci nákladů.

Popis položky	**Jednotkové náklady**	**Náklady celkem**
Překlad informování o správci	250 Kč	250 Kč
6x 300 x 200mm tabulka s piktogramem	54,45 Kč	326,7 Kč
6x 200 x 100 mm tabulka s informacemi o správci	21,78 Kč	130,7 Kč
1x Poštovné	90 Kč	90 Kč
Objednávka a instalace tabulek zaměstnancem společnosti XYZ a.s. (2 h)	170 Kč	340 Kč
Celkem		**1137,4 Kč**

Tab. 1: Kalkulace nákladů na správné označení budov
Zdroj cen: interní zdroj, tabulky a poštovné: Safetyshop (2017)

Případná sankce v tomto případě již není tak jednoznačná jako v předchozím bodě, a také nebyla nalezena žádná předchozí judikatura zaobírající se touto

tematikou. Vybízí se klasifikace jako delikt dle § 45 odst. 1 písm. f) ZoOÚ, kdy správce „neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem“, neboť dle § 11 odst. 1 ZoOÚ je správce povinen subjekt údajů při shromažďování osobních dat informovat o tom, kdo bude osobní údaje zpracovávat, což se bez informační tabulky vedle piktogramu kamerového záznamu neděje. Za takový delikt pak hrozí pokuta s maximální hranicí 5 000 000 Kč.

5.3 Zkrácení doby uchovávání kamerových záznamů

Společnost XYZ a.s. v současné době na svých serverech uchovává záznamy z kamerových systémů po dobu 30 dnů. Účelem kamerového monitorování je u společnosti XYZ a.s. ochrana majetku správce a třetích osob. Záznamy z kamer jsou pak kontrolovány jen v případě, že se stane nějaký bezpečnostní incident. Takovým incidentem může být odcizení majetku z prostor zaměstnavatele, nebo neoprávněné vniknutí do prostor zaměstnavatele.

Zákon ochraně osobních údajů stanovuje lhůtu pro uchování kamerových záznamů jako dobu nezbytnou pro naplnění účelu zpracování těchto kamerových záznamů. Ve své tiskové zprávě pak Úřad zmiňuje dobu nepřesahující několik dnů. Horký (2013) například uvádí, že sedmidenní doba uchovávání záznamu v hotelu za účelem ochrany majetku se jeví jako neúměrná stanovenému účelu. Šebesta (2016) pak uvádí, že jakékoliv ukládání kamerového záznamu přesahující tři dny požaduje Úřad vždy racionálně zdůvodnit.

Na jakou dobu má společnost XYZ a.s. povoleno uchovávat záznamy z registru zpracování osobních údajů vyčíst nelze, a ani společnost samotná se k tomuto tématu nevyjádřila. Pádným argumentem pro delší lhůtu může být fakt, že například odcizení nějakého hardware zaměstnancem nemusí být rozpoznáno ihned a prozkoumání starších záznamů by později mohlo odhalit pachatele. Je však zcela na uvážení Úřadu, zda to bude pádný argument i pro něj. Společnost XYZ a.s. by problematiku zkrácení doby uchovávání kamerových záznamů měla zvážit a také probrat s Úřadem, aby se ujistila, že se nedopouští deliktu uchování osobních údajů po dobu delší než nezbytnou k naplnění účelu zpracování dle § 45 odst. 1 písm. d) ZoOÚ, za který hrozí pokuta do výše 5 000 000 Kč.

Případné zkrácení doby uchovávání kamerových záznamů se v nákladech firmy neprojeví.

5.4 Úprava souhlasu se zpracováním osobních údajů

V rámci problematiky souhlasu se zpracováním osobních údajů se společnost XYZ a.s. nedopouští žádného prohřešku vůči platné legislativě, nicméně by si jeho lehkou úpravou mohla ulehčit případné hledání nových zaměstnanců.

Pokud uchazeč zareaguje v současné době na pracovní nabídku přes webový portál Jobs.cz nebo Jobote.com, společnost XYZ a.s. má právo s jeho osobními údaji nakládat po dobu tří let i za účelem zařazení do databáze potenciálních zaměstnanců. Pokud však uchazeč zareaguje přes kariérní stránku společnosti

XYZ a.s., která je součástí její webové prezentace, souhlasí v tomto případě pouze se zpracováním osobních údajů v maximální délce jednoho roku, a to pouze za účelem výběrového řízení. Společnost XYZ a.s. v tomto případě musí po ukončení výběrového řízení veškeré osobní údaje uchazečů zlikvidovat.

Společnost XYZ a.s. by mohla sjednocením podmínek s portály Jobs.cz a Jobote.com začít uchovávat osobní údaje uchazečů za účelem jejich zařazení do evidence potenciálních uchazečů. Pomohlo by jí to zejména při výběrovém řízení na vyšší pozice, na které společnost XYZ a.s. ukládá obecně náročnější požadavky. Pokud by se například stalo, že nový zaměstnanec neprojde zkušební dobou, společnost XYZ a.s. by se mohla v krátké době ozvat kandidátům, kteří o danou pozici měli zájem, ale nakonec nebyli vybráni. Odpadlo by tak, v současné době nutné, opakované zveřejnění inzerátů nabízených pracovních míst a obnovení výběrového řízení od začátku. Stejně by pak mohla společnost postupovat při vytvoření nového pracovního místa, na které by se hodil některý z předchozích uchazečů. Společnost XYZ a.s. by pak také nemusela rozlišovat zpracování osobních údajů uchazeče podle toho, zda uchazeč zareagoval na nabízené pracovní místo skrze jeden z webových portálů patřících pod společnost LMC s.r.o., nebo z kariérní stránky společnosti XYZ a.s.

Úpravou současného souhlasu se zpracováním osobních údajů by výsledný souhlas mohl vypadat následovně:

„Souhlasím se zpracováním a uchováním osobních údajů ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů v platném znění pro účely výběrového řízení na obsazení volné pracovní **pozice a dále pro účely evidování mé osoby jakožto potenciálního zaměstnance. Souhlas uděluji na dobu 3 roky ode dne odeslání osobních údajů.** Současně potvrzuji, že osobní údaje uvedené v životopise jsou pravdivé a přesné."

Jako druhá úprava se nabízí lokalizace souhlasu se zpracováním osobních údajů na webovém portálu společnosti XYZ a.s. do češtiny v případech, kdy je inzerát uveden v českém jazyce a od uchazeče se tak neočekává důkladná znalost angličtiny. V současné době musí takový uchazeč souhlasit s anglickou verzí, které nemusí rozumět. Současný souhlas se zpracováním osobních údajů společnost XYZ a.s. do češtiny přeložený má, jelikož ho dává uchazeči podepsat v papírové formě při příchodu na pracovní pohovor. Překlad by se tak týkal pouze změněné části souhlasu. Aby se nemusela upravovat administrace kariérní stránky pro rozpoznání, zda je inzerát v českém nebo anglickém jazyce, společnost XYZ a.s. může u inzerátů na své kariérní stránce uvést souhlas se zpracováním osobních údajů v obou jazykových verzích zároveň.

V rámci procesu zavedení obměněného souhlasu se zpracováním osobních údajů by musel zaměstnanec právního oddělení věnovat 4 hodiny. Nejdříve je nutné, aby se seznámil se souhlasem, který používají webové portály patřící pod společnost LMC s.r.o. a následně podle něj upravil stávající souhlas společnosti XYZ a.s. Část textu, která bude změněna, pak musí zaměstnanec poslat na překlad do angličtiny. Implementaci do kariérní stránky společnosti XYZ a.s. provede webový administrátor, kterému tato akce nebude trvat více než hodinu.

Popis položky	Jednotkové náklady	Náklady celkem
4 h zaměstnance z právního oddělení	240 Kč	960 Kč
Překlad části textu	250 Kč	250 Kč
1 h zaměstnance IT	200 Kč	200 Kč
Celkem		**1410 Kč**

Tab. 2: Kalkulace nákladů na úpravu souhlasu se zpracováním osobních údajů
Zdroj: Interní zdroj

5.5 Sjednocení informací týkajících se povinnosti aktualizovat osobní údaje

Poslední drobnou nesrovnalostí v dokumentaci společnosti XYZ a.s. je rozdílně uvedená doba, za jakou musí zaměstnanec oznámit změnu ve svých osobních údajích. Takovou změnou obvykle bývá změna trvalého bydliště, rodinného stavu, či změna zdravotní pojišťovny. Zaměstnavatel musí dle § 5 odst. 1) písm. c) ZoOÚ zpracovávat přesné osobní údaje a v případě potřeby tyto údaje aktualizovat. Společnost XYZ a.s. tuto povinnost přenáší ve větší míře na své zaměstnance, kteří jsou povinni v případě změny jejich osobních údajů uvědomit zaměstnavatele. V rámci pracovního řádu je lhůta pro oznámení stanovená na osm dnů od vzniku změny. V osobním dotazníku pak zaměstnanec souhlasí s tím, že takovou změnu nahlásí maximálně do tří dnů. Tuto dobu by bylo vhodné sjednotit, aby platily jasné pravidla.

Společnosti za tuto nesrovnalost nehrozí žádný postih, neboť si tato pravidla nastavila sama a nenutí ji k tomu žádný zákon, který by porušovala. Zaměstnanec právního oddělení po sjednocení zmiňovaných lhůt může rozeslat hromadný e-mail, ve kterém změnu v pracovním řádu ohlásí. V této zprávě také mohou být zaměstnanci požádání, aby si své osobní údaje zkontrolovali a ti co na ohlášení změny dříve zapomněli, tak budou moci učinit. Čas nutný ke změně údaje v rámci pracovního řádu je zanedbatelný a dohromady s rozesláním hromadného e-mailu by neměl trvat více než hodinu, tudíž by náklady na tento návrh firmu neměly převýšit 240 Kč, což je přepočtená mzda zaměstnance právního oddělení na hodinu.

6 Diskuze

Aby vůbec mohla společnost zpracovávat osobní údaje, musí tuto činnost, až na výjimky stanovené zákonem, oznámit Úřadu a následně pak zpracování osobních údajů podřídit zejména zákonu 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů. Společnost XYZ a.s. sice nemá pro zacházení s osobními daty subjektů specifickou směrnici, nicméně má jednotlivé práva a povinnosti vyplývající ze ZoOÚ zanesené v ostatní dokumentaci. Zmínky tak lze nalézt jako součásti pracovní smlouvy, smlouvy o mzdě, osobního dotazníku, pracovního a mzdového řádu a v neposlední řadě také v řádu skartačním. Dikce zákona neudává povinnost vedení samostatné směrnice týkající se ochrany osobních údajů a jednání společnosti XYZ a.s. je tak v tomto případě v pořádku.

Otázkou však je, zda takovou směrnici nebude nutné vytvořit s příchodem obecného nařízení o ochraně osobních údajů (GDPR), které vstoupí v platnost 25. 5. 2018. Subjektům vzniknou nová práva, jmenovitě například právo na výmaz, právo na přenositelnost údajů či právo vznést námitku proti zpracování. Nejen že budou muset být zaměstnanci zpracovávající osobní údaje pečlivě o GDPR proškoleni, ale zároveň by jim určitě pomohlo, pokud budou mít jednotný dokument s jasnými postupy, jak v případě požadavků subjektů údajů reagovat na jednotlivé akce, které subjektům údajů GDPR nově umožňuje. Nové však jsou nejen práva subjektu údajů, ale i povinnosti správců. Nově musí správci u zpracování, které by mohl být rizikové, provádět posouzení dopadu na ochranu osobních údajů a toto posouzení konzultovat s dozorovým orgánem, vést záznamy o zpracování osobních údajů a také ohlašovat případy narušení bezpečnosti osobních údajů. Pro zavedení vnitropodnikové směrnice věnující se ochraně osobních údajů hovoří i navýšení sankcí za případné porušení nařízení GDPR. Již za méně závažné porušení může společnost XYZ a.s. čelit pokutě až ve výši 10 000 000 EUR, což je více než padesátinásobek současné horní hranice pokuty za méně závažný správní delikt.

V současné době má však společnost XYZ a.s. značný problém v povinném oznámení o zpracování osobních údajů Úřadu. Po změně právní formy, sídla a s tím spojenou změnou IČO, společnost XYZ a.s. opomněla ukončit původní registraci a podat na stránkách Úřadu registraci novou. To však není jediným prohřeškem v rámci oznamovací povinnosti Úřadu. Společnost XYZ a.s. má v registraci uvedeno, že bude zpracovávat pouze adresní a identifikační údaje, nicméně zpracovává i údaje popisné. Dalším pochybením je pak neuvedení dalších míst, kde probíhá zpracování osobních údajů. Společnost XYZ a.s. má v současné době několik poboček, kde se zpracovávají osobní údaje, a je tedy nutné, aby je v rámci registrace uvedla. Posledním rozporem v současné registraci pak je uvedení faktu, že osobní údaje zaměstnanců nebudou předávány do zahraničí. V rámci společnosti XYZ a.s. se běžně stává, že zaměstnanci mají manažery z jiného státu a ti mají v rámci společnosti XYZ a.s. pravomoc přistupovat k osobním údajům těchto zaměstnanců. Nápravu tohoto problému není možné řešit pouze uvedením předání osobních údajů do jiných států v rámci

registrace u Úřadu, ale správce musí také požádat Úřad o povolení k této činnosti, kde musí rozvést, do jakých zemí budou osobní údaje směřovat, s jakým cílem, jaké osobní údaje budou předávány a jejich původ. Jakýkoliv z těchto deliktů je dle platné legislativy možné pokutovat až do výše 5 000 000 Kč. V praxi by pravděpodobně v tomto případě byly zmíněné jednotlivé delikty shrnuty do jednoho s klasifikací nesplnění oznamovací povinnosti dle ZoOÚ s horní hranicí pokuty 5 000 000 Kč.

U tohoto návrhu je však nutné zmínit, že s počátkem platnosti nařízení GDPR končí oznamovací povinnost správců. Uvedený návrh tedy bude mít krátkodobé trvání. To však nemění nic na tom, že současný stav společnosti XYZ a.s. porušuje nyní platnou legislativu v několika oblastech a společnost tak může být do 25. 5. 2018 pokutována až do výše 5 000 000 Kč. Vzhledem k nízké nákladovosti zrealizování návrhu je společnosti výrazně doporučeno tento návrh uskutečnit.

První momentem, kdy společnost XYZ a.s. zpracovává osobních údaje subjektů, je příležitost výběrového řízení. Osobní údaje uchazečů pak přichází hlavně z pracovních portálů Jobs.cz a Jobote.com, a dále z kariérní stránky společnosti XYZ a.s. Z ostatních zdrojů uchazeči zpravidla nepřicházejí. Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů, a tak se, nehledě na umístění inzerátu s volným místem, pod každým inzerátem nachází svolení ke zpracování osobních údajů, se kterým uchazeč musí před zareagováním na daný inzerát souhlasit. Společnost XYZ a.s. tak v tomto případě jedná zcela v souladu s právním řádem. I přes bezchybné chování vůči platné legislativě by však získávání souhlasu mohlo fungovat lépe. Jak bylo navrženo v předchozí kapitole, společnost XYZ a.s. by sjednocením svého současného souhlasu se zpracováním osobních údajů se souhlasem používaným na portálech Jobs.cz a Jobote.com mohla uchovávat životopisy za účelem evidence potenciálních zaměstnanců. Společnost XYZ a.s. by pak mohla lehčeji oslovovat schopné uchazeče, kteří sice nebyli v rámci předchozích výběrových řízení vybráni na danou pozici, ale přesto mohou svými kvalitami vynikat jinde. S naplněnou evidencí potenciálních zaměstnanců by se také měl urychlit průběh výběrového řízení, kdy při vytvoření nového místa nebude třeba čekat, až daný inzerát uchazeči najdou a zareagují na něj, ale personalisté společnosti XYZ a.s. by mohli proaktivně začít dřívější uchazeče oslovovat sami. V některých případech by tak inzerát nemuseli vůbec zveřejňovat. Souhlas se zpracováním osobních údajů by pak firma mohla na svých stránkách uvádět jak v anglickém, tak i v českém jazyce. V současné době se může stát, že uchazeč reagující na pracovní nabídku uvedenou v češtině na kariérní stránce společnosti bude muset souhlasit s něčím, čemu nemusí porozumět. Vzhledem k zaměření společnosti XYZ a.s. na jazykové služby by jim zajištění potřebného překladu nemělo činit žádnou obtíž.

Proces výběrového řízení ve společnosti XYZ a.s. následně probíhá bez jakéhokoliv rozporu s právním řádem. Uchazeči je při příchodu do budovy dán k znovu k podpisu souhlas se zpracováním osobních údajů, aby společnost XYZ a.s. měla zpracování osobních údajů kryto fyzickým důkazem souhlasu. Během výběrového řízení nejsou po uchazečích vyžadovány žádné citlivé osobní

údaje, ani žádné další osobní údaje, které by byly v rozporu s účelem pro výběrové řízení. Po ukončení výběrového řízení jsou veškeré osobní údaje neúspěšných uchazečů zařazeny k výmazu a skartaci, neboť pominul jejich stanovený účel pro výběrové řízení. Společnost XYZ a.s. likviduje také osobní údaje uchazečů získané přes webové portály Jobs.cz a Jobote.com, i přesto že by je mohla uchovávat po dobu tří let i za účelem evidence potenciálních zaměstnanců. Přístup společnosti XYZ a.s. k průběhu výběrového řízení by se dal hodnotit jako velmi obezřetný a je plně v souladu s právním řádem.

Zaměstnavatel při přijetí nového zaměstnance zakládá jeho osobní spis, ve kterém se uchovávají veškeré vniklé dokumenty se zaměstnancovým jménem. Osobní spis je veden jak v listovní, tak i v elektronické podobě. Mezi prvními dokumenty se tam dostává osobní dotazník, který musí zaměstnanec vyplnit před podepsáním pracovní smlouvy. Tento dotazník obsahuje pouze nejnutnější identifikační a adresní údaje. Osobní spis obsahuje také potvrzení o zdravotní způsobilosti zaměstnance, který ovšem dle legislativy není brán jako citlivý údaj. Veškeré uchovávané dokumenty mají svůj účel a jsou uchovávány dle zákona.

Bezpečnost listinných dokumentů je zajištěna jednak jejich uchováním v místnosti, kam mají přístup pouze pracovníci personálního oddělení pomocí čipové karty, za druhé jsou ve zmiňované místnosti tyto dokumenty uloženy v plechových skříních na zámek pro případ, že by se do místnosti i tak někdo dostal. Elektronická verze je pak chráněna systémem přístupových práv, přístupem pouze z předem nainstalovaného programu a počítač obecně pak heslem, které si musí každý zaměstnanec po určité době měnit, povinností zamykat počítač pokaždé, když od něj zaměstnanec odchází a také aktuálním antivirovým programem. Ochrana osobních údajů je tak v rámci možností dostačující.

Jakoukoli změnu v osobních údajích zaměstnance je zaměstnanec dle vnitřních předpisů povinen oznámit zaměstnavateli. V rámci předpisů společnosti XYZ a.s. však není jednoznačně uvedeno, do kdy musí tato akce být provedena. Osobní dotazník říká nejpozději do tří dnů, pracovní řád pak udává dnů osm. Společnost by tyto lhůty měla upravit změnou v jednom z uvedených dokumentů. Při této příležitosti by měla změnu oznámit všem zaměstnancům, což jim povinnost aktualizovat svoje osobní údaje připomene a může se tak zvýšit celková aktuálnost osobních údajů.

Bezchybně také společnost XYZ a.s. postupuje při práci s fotografiemi.

Co se týče soukromí zaměstnanců, jeho potenciální narušení může vzniknout sledováním pomocí kamerového systému, monitorováním e-mailové pošty, přístupů na internet, služebních telefonů a automobilů. Automobil však nemá přidělen žádný ze zaměstnanců společnosti XYZ a.s. a tuto variantu lze tak ihned vyloučit.

Kamerový systém má společnost dle zákona nahlášený v rámci registrace u Úřadu. Samotné kamery má nastaveny tak, že soukromí zaměstnanců na pracovišti žádným způsobem nenarušují. Problémem je však nedostatečné označení na jedné z budov společnosti XYZ a.s., kdy je piktogram oznamující monitorování pomocí kamerového systému umístěn příliš vysoko a zaměstnanci by si ho nemuseli všimnout a zároveň zde chybí bližší údaje o kamerovém systému

a správci. Tento problém však nemůže narušit ničí soukromí, ale týká se pouze pochybení v informační povinnosti. Společnost by měla věnovat pozornost i době uchovávání záznamu, neboť současných 30 dní se zdá oproti vyjádření Úřadu, kdy by délka uchování záznamu neměla přesáhnout pár dní, nepřiměřené. Společnost by se se současnou dobou mohla dopouštět uchovávání osobních údajů po delší dobu, než je nezbytné. Tato skutečnost však nemusí být ve skutečnosti chybou, neboť 30-denní lhůtu uložení kamerových záznamů by si mohla firma ponechat, pokud jí to schválí Úřad.

V rámci monitorování služebních telefonů, e-mailové pošty a přístupů na internet společnost XYZ a.s. jedná bezchybně.

Stejně tak bezchybně jedná společnost XYZ a.s. v oblasti zpracovávání osobních údajů i po ukončení pracovního poměru. Veškeré dokumenty bývalého zaměstnance putují ke skartaci či archivaci dle skartačního řádu, který je upraven dle platné legislativy.

Celkově je možné uvést, že samotný stav ochrany osobních údajů a soukromí je ve společnosti XYZ a.s. na dobré úrovni. Nebyl nalezen žádný problém, který by významně ohrožoval osobní údaje nebo soukromí subjektů. Pochybení, kterých se společnost XYZ a.s. jsou většinou administrativního charakteru, které se subjektů údajů nijak nedotkne.

7 Závěr

Obsahem této diplomové práce byla problematika ochrany osobních údajů a soukromí. Tato problematika byla blíže aplikována na oblast pracovněprávních vztahů. Cílem bylo na základě podrobné analýzy úrovně ochrany soukromí a osobních údajů v konkrétním obchodním závodu, v našem případě XYZ a.s., po porovnání s platnou právní úpravou České republiky vytvořit konkrétní opravná opatření, která by obchodnímu závodu zajistila soulad jejich počínání s legislativou České republiky. Vymezení důsledků porušování povinností při zpracování osobních údajů a ochrany soukromí, stejně tak jako vyčíslení ekonomické náročnosti zavedení jednotlivých návrhů jsou součástí návrhů.

V rámci literární rešerše jsou představeny nejdříve právní prameny týkající se ochrany osobních údajů, jejich vývoj a hlavní principy. Poté jsou vymezeny důležité pojmy jako osobní údaj, zpracování, subjekt údajů, správce a zpracovatel, které jsou následně využívány v celé práci a je tedy nezbytné je pochopit. Rešerše se věnuje také Úřadu pro ochranu osobních údajů, jakožto jedinému dozorovému orgánu v České republice, který dohlíží na dodržování povinností pramenících ze zákona o ochraně osobních údajů a také vede registr zpracování osobních údajů. Představeny jsou také sankce, které hrozí jak fyzickým, tak i právnickým osobám, které by jednaly v rozporu se zmiňovaným zákonem.

Další oblastí je pak ochrana soukromí, kde je vysvětlen samotný pojem soukromí a je nastíněno jeho zakotvení v právních pramenech. Podrobněji se pak práce věnuje problematice monitorování zaměstnanců, jaké mají v tomto případě zaměstnanci právo na soukromí a jak jim může být zaměstnavatelem narušováno. Zmíněná problematika je zde aplikována v kontextu sledování kamerovými systémy, kontrolování zaměstnancových přístupů na internet, jejich e-mailové korespondence na pracovišti, přidělených telefonů a služebních automobilů.

Zařazena byla také problematika nového nařízení o ochraně osobních údajů (GDPR), neboť od 25. května 2018 vstupuje toto nařízení v účinnost a mění výrazně dosavadní přístup k ochraně osobních údajů.

Vlastní práce se věnuje analýze úrovně ochrany osobních údajů ve společnosti XYZ a.s. od počátku výběrového řízení až po nakládání s osobními údaji po ukončení pracovního poměru. Výsledky analýzy procesů ve společnosti XYZ a.s. jsou zde porovnávány s platnou legislativou České republiky, což následně bylo zdrojem pro dále uvedené návrhy.

Bylo zjištěno, že společnost XYZ a.s. nejedná zcela v souladu s platnou legislativou. Mezery byly nalezeny zejména v administrativních povinnostech vůči Úřadu. Nejzávažnějším problémem byl stav registrace v registru zpracování osobních údajů. Společnost XYZ a.s. po změně sídla a právní formy neukončila registraci zpracování osobních údajů u zaniklé právní formy společnosti a také neoznámila zpracování osobních údajů u formy nové. V současné době tak společnost nesplňuje nejzákladnější princip ochrany osobních údajů a to oznamo-

vací povinnost Úřadu. Problémy byly nalezeny i v dalších částech registrace, neboť společnost zpracovává i kategorii údajů, kterou v registraci neuvedla, provádí zpracování na místech, které v registraci nemá uvedené a také předává osobní údaje zaměstnanců do zahraničí i přes vyslovené uvedení, že takto s osobními údaji nakládáno nebude. Dále byl objeven rozpor s metodikou Úřadu týkajících se kamerových systémů.

Na všechny nalezené problémy byly vytvořeny návrhy, které by měly uvést nesrovnalosti do souladu s platnou právní úpravou České republiky, včetně vyčíslení případných sankcí a kalkulací na zavedení jednotlivých návrhů. V rámci diskuze pak byly shrnuty jednotlivé návrhy a některé z nich vzaty do úvahy s novým nařízením GDPR. Kromě nápravy problémů byly také navrženy doporučení, které by společnosti XYZ a.s. mohly pomoci v pracovněprávním procesu.

Tato práce objevila několik problémů, jejichž náprava nebude nijak zvlášť nákladná a zároveň se zavedením uvedených návrhů společnost vyhne případným sankcím, jejichž výše rozhodně není zanedbatelná. Informace z této práce mohou využít k vlastnímu prospěchu i ostatní obchodní závody, neboť je v této práci problematika ochrany osobních údajů a soukromí přehledně shrnuta a je poukázáno na některé nejčastější prohřešky, kterých se mohou, většinou nevědomě, dopouštět i ostatní společnosti.

8 Literatura

BARENDT, ERIC. *Privacy and freedom of speech*. In: Kenyon, Andrew T., Richardson, Megan. New dimensions in privacy law: international and comparative perspectives. 1st pub. Cambridge: Cambridge University Press, 2006. 296 s. ISBN 0-521-86074-1.

BARTÍK, VÁCLAV. *Zákon o ochraně osobních údajů s komentářem*. Olomouc: Anag, 2010. Právo (Anag). ISBN 9788072636136.

BARTÍK, VÁCLAV A EVA JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5.

BARTÍK, VÁCLAV A EVA JANEČKOVÁ. *Ochrana osobních údajů v životě podnikatele : 103 řešení modelových situací*. 1. vyd. Olomouc: ANAG, 2013. 199 s. ISBN 978-80-7263-811-6

BARTOLINI, CESARE, ET AL. *Assessing IT Security Standards Against the Upcoming GDPR for Cloud Systems* [online]. 2015 [cit. 2017-03-26]. Dostupné z: http://hdl.handle.net/10993/20791

BURIAN, DAVID A ZUZANA RADIČOVÁ. K *některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR)*. In: Právní prostor [online]. 2016 [cit. 2017-03-26]. Dostupné z: https://goo.gl/cp3Wto

DUŠEK, VIKTOR. *GDPR: Přehled nejvýznamnějších změn*. In: KPMG|CZ [online]. 2017 [cit. 2017-03-26]. Dostupné z: https://goo.gl/Mv1Jvl

EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA. *Evropská úmluva o ochraně lidských práv*. [online]. [cit. 2017-03-25]. Dostupné z: https://goo.gl/Tn5yuF

FIALOVÁ, EVA. *Bezkontaktní čipy a ochrana soukromí*. Praha: Leges, 2016. Praktik. ISBN 978-80-7502-150-2.

GUTWIRTH, SERGE. *Privacy and the information age*. Lanham, Md.: Rowman & Littlefield Publishers, 2002. ISBN 9780742517462.

HEIMES, RITA A SAM PFEIFLE. *Study: GDPR's global reach to require at least 75,000 DPOs worldwide*. In: International Association of Privacy Professionals [online]. 2016 [cit. 2017-03-27]. Dostupné z: https://goo.gl/gfsmf1

HORKÝ, ŠTĚPÁN. *Kamerové systémy – dobrý pomocník, ale …* In: Epravo.cz [online]. 2013 [cit. 2017-05-09]. Dostupné z: https://goo.gl/6aIohg

HRDLÍK, MARTIN. *Konec legendárního 101/2000 Sb.* In: KPMG|CZ [online]. 2016 [cit. 2017-03-26]. Dostupné z: https://goo.gl/8Qn6yZ

JANEČKOVÁ, EVA. *Nejčastější pochybení zaměstnavatelů při plnění povinností dle zákoníku práce*. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-518-4.

JANEČKOVÁ, EVA A VÁCLAV BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3.

KADLECOVÁ, TEREZA, 2015. *GPS ve služebních vozidlech aneb malý čip = velká komplikace*? Praktická personalistika. Anag, 2015(3-4). [online]. [cit. 2017-19-03]. Dostupné z: https://goo.gl/Rzk9rW

KOLMAN, PETR. *Právo na informace*. Brno: Masarykova univerzita, 2010. Edice učebnic PrF MU. ISBN 978-80-210-5135-5

Listina základních práv a svobod. In: Ústavní zákon č. 2/1993 Sb. ve znění ústavní-ho zákona č. 162/1998 Sb. 1992. [cit. 2017-03-25]. Dostupné z: https://zakonyprolidi.cz/cs/1993-2

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

MATES, PAVEL, EVA JANEČKOVÁ A VÁCLAV BARTÍK. *Ochrana osobních údajů*. Praha: Leges, 2012. Praktik. ISBN 978-80-87576-12-0.

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

MORÁVEK, JAKUB. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť. ISBN 978-80-7478-139-1.

Nález Ústavního soudu České republiky ze dne 12. 4. 1994, sp. zn. Pl. ÚS 4/94, [cit. 2017-17-03]. Dostupné z: http://kraken.slv.cz/Pl.US4/94

Nález Ústavního soudu České republiky ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99, [cit. 2017-10-03]. Dostupné z: http://kraken.slv.cz/II.US517/99

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. In: EUR-Lex [online]. [cit. 2017-03-25]. Dostupné z: https://goo.gl/o4nPdu

NEUWIRT KAREL. *Ochrana osobních údajů a vstup do EU*. In: Data Security Management [online], 2003(6) [cit. 2017-03-22]. Dostupné z: https://goo.gl/ucQzKG

PATÁK, TOMÁŠ. *GDPR a role ÚOOÚ*. In: Úřad pro ochranu osobních údajů [online]. 2017 [cit. 2017-03-26]. Dostupné z: https://goo.gl/Cu1Zsf

PAVLÁT, DAVID. K *dodržování povinnosti přijmout a provést bezpečností opatření k ochraně osobních údajů v soukromoprávní sféře*. In: Úřad pro ochranu osobních údajů [online], 2013 [cit. 2017-03-23]. Dostupné z: https://goo.gl/fG76IV

SAFETYSHOP: *Bezpečnostní značení, výrobky pro bezpečnost* [online]. 2017 [cit. 2017-05-08]. Dostupné z: http://www.safetyshop.cz/

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: eur-lex.europa.eu [online]. 2015 [cit. 2015-11-22]. Dostupné z: https://goo.gl/YfYZoc

SOBEK, TOMÁŠ. *Svoboda a soukromí*. In: Šimíček, Vojtěch. Právo na soukromí. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. Sborníky. ISBN 978-80-210-5449-3.

ŠEBESTA, KAMIL. *Využívání kamerového systému z pohledu zákona o ochraně osobních údajů*. In: eLAW - právní portál [online]. [cit. 2017-05-13]. Dostupné z: https://goo.gl/uMGQrY

ŠKORNIČKOVÁ, EVA. *DPO ochrání firmu i její klienty*. In: GDPR.cz [online]. 2017 [cit. 2017-03-27]. Dostupné z: https://goo.gl/xKO769

Úmluva č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. ledna 1981. In: Council of Europe [online]. [cit. 2017-03-25]. Dostupné z: https://goo.gl/URBWys

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Ochrana osobních údajů: vybrané otázky: příručka pro podnikatele*. Brno: Masarykova univerzita, 2011. ISBN 978-80-210-5572-8.

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Provozování kamerových systémů*. Brno: Masarykova univerzita, 2012. ISBN 978-80-210-6017-3.

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Tisková zpráva 26. 1. 2006*. In: Úřad pro ochranu osobních údajů [online]. [cit. 2017-04-07]. Dostupné z: https://goo.gl/G6TG8P

VARVAŘOVSKÝ PAVEL. *Se záznamem či bez záznamu*. In: Informační bulletin [online], Úřad pro ochranu osobních údajů, 2011(2) [cit. 2017-03-22]. Dostupné z: https://goo.gl/YLqiYI

VIDRNA JAN A ZDENĚK KOUDELKA. Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7.

WARREN, SAMUEL A LOUIS BRANDEIS. *The Right to Privacy*. Harvard Law Review, 1890 [online]. [cit. 2017-10-03]. Dostupné z: https://goo.gl/Sy8oaJ

WESTIN, ALAN F.. *Privacy and freedom*: chairman of the special committee on science and law, the association of the bar of the city of New York. New York: Atheneum, 1967.

Zákon č. 89/2012 Sb., občanský zákoník. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89

Zákon č. 40/2009 Sb., trestní zákoník. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

Zákon č. 111/2009 Sb., o základních registrech. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-111

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://zakonyprolidi.cz/cs/2000-133

Zákon č. 200/1990 Sb., České národní rady o přestupcích. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/1990-200

Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-250

Zákon č. 255/2012 Sb., o kontrole (kontrolní řád). In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-255

Zákon č. 262/2006 Sb., zákoník práce. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-262

Zákon č. 468/2011 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích. In: Portál veřejné zprávy [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://goo.gl/z5RUH9

Zákon č. 586/1992 Sb., Zákon České národní rady o daních z příjmů. In: Zákony pro lidi.cz [online]. 2016 [cit. 2017-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/1992-586