Mendelova univerzita v Brně
Provozně ekonomická fakulta

Ochrana soukromí a ochrana osobních údajů zaměstnance v obchodní společnosti

Diplomová práce

Vedoucí práce:

JUDr. Hana Kelblová, Ph.D.

Bc. Veronika Zezulová

Brno 2020

Tímto bych ráda poděkovala vedoucí diplomové práce paní JUDr. Haně Kelblové, Ph.D. za vstřícnost, cenné připomínky a odborné rady, které mi pomohly při zpracování této práce. Dále bych chtěla poděkovat zaměstnancům útvaru Personalistika a mzdy společnosti XX a. s. za vstřícný přístup a poskytnutí informací potřebných pro tuto práci.

Čestné prohlášení

Prohlašuji, že jsem práci **Ochrana soukromí a ochrana osobních údajů zaměstnance v obchodní společnosti** vypracovala samostatně a veškeré použité prameny a informace uvádím 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 závěrečných prací.

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

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity, 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 3.1.2020 .....

Abstract

Zezulová, V. Protection of Privacy and Personal data of Employees in a Business Organization. Diploma thesis. Brno: Mendel University in Brno, 2020.

The diploma thesis is focused on the protection of privacy and personal data in labour relations. The literature research is devoted to the definition of basic terms, the legal base of the protection of personal data and privacy, the rights and obligations of the parties, the supervisory authority and the sanctions related to the non-compliance of obligations imposed by the law. The research focuses on the conflict of interest of the employer and the right to privacy of the employee and the degree of legitimacy of workplace monitoring.

The original research part deals with the analysis of personal data protection and privacy measures in the chosen business organization during the whole process from the beginning of the selection process, during the duration of the employment relationship to its termination. Subsequently, the ways of monitoring employees and their legitimacy are evaluated. Based on analysed facts, corrective recommendations, including the economic aspect, are proposed in conclusion of the thesis.

Keywords

personal data, privacy, data administrator, data subject, The office for Personal Data Protection, The General Data Protection Regulation, employees monitoring

Abstrakt

Zezulová, V. Ochrana soukromí a ochrana osobních údajů zaměstnance v obchodní společnosti. Diplomová práce. Brno: Mendelova univerzita v Brně, 2020.

Diplomová práce je zaměřena na problematiku ochrany soukromí a ochrany osobních údajů v pracovněprávních vztazích. Literární rešerše je věnována vymezení základních pojmů, právnímu zakotvení ochrany osobních údajů a soukromí, právům a povinnostem zúčastněných stran, dozorovému úřadu a sankcím spojených s nedodržováním povinností. Rešerše se zaměřuje na střet zájmů zaměstnavatele a práva na soukromí zaměstnance a míru oprávněnosti monitoringu pracoviště.

Vlastní práce se zabývá analýzou postupů ochrany osobních údajů a soukromí ve vybrané obchodní společnosti v rámci celého procesu od počátku výběrového řízení, v průběhu trvání pracovněprávního vztahu až po jeho ukončení. Následně je pozornost věnována oprávněnosti monitoringu pracoviště a jednotlivých zaměstnanců. Na závěr jsou na základě analýzou zjištěných nedostatků navržena nápravná opatření včetně ekonomického aspektu.

Klíčová slova

osobní údaj, soukromí, správce údajů, subjekt údajů, Úřad pro ochranu osobních údajů, Obecné nařízení o ochraně osobních údajů, monitoring zaměstnanců

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

BOZP	Bezpečnost a ochrana zdraví při práci
ČR	Česká republika
EU	Evropská unie
GDPR	Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
HR	oddělení lidských zdrojů (human resources)
LZPS	Listina základních práv a svobod
NOZ	Zákon č. 89/2012 Sb., občanský zákoník ve znění pozdějších předpisů
OSSZ	Česká správa sociálního zabezpečení
ÚOOÚ	Úřad na ochranu osobních údajů
ZoOOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisu
ZoZ	Zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů
ZP	Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

1 Úvod

Osobní údaje a jejich zpracování, ochrana soukromí, monitoring, to jsou pojmy, se kterými se setkáváme denně, a v dnešní době jsou často řešeny. Tématem této práce je ochrana soukromí a ochrana osobních údajů zaměstnance v obchodní společnosti.

Osobní údaje, informace a soukromí jsou s člověkem spojeny po celý jeho život. Už po narození člověk získá první osobní údaje, jako je jméno, příjmení, datum a místo narození. Dále je dítěti přiděleno rodné číslo, které slouží po zbytek jeho života jako jedinečný identifikátor, a proto je velmi citlivým údajem. S postupem života se nabalují další údaje, například bydliště, vzdělání, rodinný a zdravotní stav. Tyto osobní údaje člověka identifikují, odlišují ho od ostatních a vytváří jeho osobnost. Osobními údaji nejsou jen ty, které identifikují, ale i ty, které se identifikovaných osob týkají, čímž činí člověka ve společnosti lidí jedinečným.

Osobní údaje nejsou věcí novou, naopak jsou záležitostí velice starou. Dá se říct, že provázejí lidskou společnost od počátku její existence, avšak pozornosti, a především ochrany, se jim dostává jen několik desetiletí (Mates, 2012). Důvodem je především rozvoj společnosti a techniky, se kterým souvisí růst hodnoty informací, kam pochopitelně patří i osobní údaje.

V dnešní době je téma ochrany osobních údajů velmi aktuální. Jedním z důvodů je vyspělost informačních technologií a tím je dána rychlost přenosu informací, kdy získat osobní informace o člověku a zneužít je, je jednodušší než kdy dřív. I když technologický pokrok a nové vynálezy usnadnily člověku pracovní i soukromý život, přinesly ovšem také velký zásah do soukromí, na což nebyli lidé v dřívějších dobách zvyklí. Přinesly riziko a ohrožení bezpečnosti, s čím se musí společnost vyrovnat. I přesto se mnoho lidí stále dívá na ochranu osobních údajů jako na něco zcela zbytečného a obtěžujícího.

Bohužel mnoho osob nakládá se svými osobními údaji lehkovážně, neuvědomují si rizika s tím spojená. Tím usnadňují pozici subjektům, pro něž jsou takové informace cenné a mohou je využít, v horším případě zneužít, např. v obchodním styku. Lidé by měli se svými údaji nakládat rozvážně, poskytovat je jen v případech, kdy je to nutné a stejně tak si chránit své soukromí.

Soukromí jedince je narušováno sociálními sítěmi. Sítě nabývají na popularitě především u mladších generacích. Lidé by si měli dobře rozmyslet, které informace o své osobě zveřejní, internet má totiž dlouhou paměť a jednou zveřejněná informace nelze už tak jednoduše vzít zpět. Někteří jedinci si svého soukromí dostatečně neváží a nechávají do něho často proniknout stovky i tisíce jiných lidí.

Zpracování osobních údajů právo na soukromí člověka výrazně narušuje, a to jak na základě zákonem stanovených důvodů, kdy musíme zpracování osobních údajů akceptovat, tak i na základě našeho souhlasu, kdy své údaje poskytujeme dobrovolně. Sotva se dá najít oblast společenského dění, kde nedochází ke zpracování osobních údajů. V moderní společnosti se zpracování osobních údajů nelze vyhnout, a proto je velmi důležité, aby byla stanovena odpovídající pravidla pro jejich zpra-

cování a také vyrovnán vztah mezi těmi, kteří osobní údaje zpracovávají a těmi, kterých se osobní údaje týkají. Je tedy důležité, aby společnost těmto pravidlům porozuměla a dodržovala je, je nutné usměrňovat tuto oblast zákonem. Jednou z nejnovějších legislativ je Obecné nařízení o ochraně osobních údajů. Nařízení značnou mírou přispělo k tomu, že je téma ochrany osobních údajů diskutovanější než kdy dřív, jelikož do značné míry nahradilo stávající zákon č. 101/2000 Sb., o ochraně osobních údajů a rozvinulo tak právní ochranu osobních údajů.

Právo člověka zadržovat informace o své osobě můžeme definovat jako soukromí. Právo na soukromí má každý jedinec bez rozdílu, a to ve všech činnostech, které provádí, tzn. i v pracovním procesu. Lidé tráví v práci značnou část svého života, proto je nutné oddělit soukromý život od toho pracovního.

V pracovněprávní oblasti platí celá řada pravidel ochrany osobních údajů. Zaměstnavatel podléhá různým povinnostem, naopak zaměstnanec má práva, která musí být dodržována. Už při hledání zaměstnání dochází k poskytování a zpracování osobních údajů, množství osobních údajů ještě narůstá po přijetí zaměstnance. Na jedné straně má zaměstnavatel právo na ochranu svého majetku, na druhé straně je zaměstnanec, který očekává šetrné nakládání s jeho soukromím a osobními údaji. Monitoring je sice velkým pomocníkem, zaměstnavatel pomocí něj chrání své zájmy, ale je to velký zásah do soukromí zaměstnance a je potřeba najít takový způsob a rozsah kontroly, aby ani jedna z těchto dvou stran nebyla poškozena.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je na základě provedené analýzy vyhodnotit úroveň ochrany soukromí a osobních údajů zaměstnanců ve vybrané obchodní společnosti, zhodnotit do jaké míry jsou dodržovány platné předpisy a nařízení v této oblasti. Následně navrhnout konkrétní opravná doporučení či zlepšení již používaných procesů respektující právní úpravu včetně ekonomického aspektu.

Dílčím cílem je vymezení pojmů souvisejících se zpracováním osobních údajů a soukromí zaměstnanců a aplikace poznatků získaných z platných právních předpisů na pracovněprávní prostředí vybrané obchodní společnosti. Analyzovat rozsah a způsob zpracování osobních údajů celé časové osy pracovního vztahu, tzn. před uzavřením pracovního poměru, v jeho průběhu a po jeho ukončení. Dále diskutovat oprávněnost monitoringu pracoviště a jednotlivých zaměstnanců a vymezit důsledky porušování povinností při zpracování osobních údajů.

Další dílčí cíl souvisí s navržením optimálního řešení postupu zpracování osobních údajů společnosti, pro posouzení zavedení tohoto řešení je důležité vyčíslení ekonomické zátěže na uvedení těchto kroků do praxe.

Předpokladem naplnění cíle je studium současné právní úpravy ochrany osobních údajů a ochrany soukromí v České republice a Evropské unii a její následná aplikace na vybranou obchodní společnost.

2.2 Metodika

Diplomová práce je rozdělena do dvou částí, a to na část literární rešerše a vlastní práce, části jsou dále členěny na jednotlivé kapitoly a podkapitoly. Na úvodní kapitoly navazuje teoretické vymezení zkoumaného problému, které shrnuje poznatky získané studiem literatury. Poznatky z teoretické části jsou aplikovány na konkrétní společnost ve vlastní práci. Následně je o výsledcích diskutováno a vše je shrnuto v závěrečné kapitole.

První částí je literární rešerše, která vychází především ze současné české a evropské legislativy, článků v odborných časopisech, komentářů k právní úpravě. Hlavním pramenem je Obecné nařízení o ochraně osobních údajů. Literární rešerše se věnuje vymezení základních pojmů ochrany osobních údajů, představen je dozorový orgán v České republice – Úřad na ochranu osobních údajů, jsou uvedeny základní práva a povinnosti zúčastněných stran a vliv nového evropského nařízení (GDPR) na tuto problematiku. Literární přehled vysvětluje, jak by měly být osobní údaje ochraňovány a dále jsou představeny možné sankce při porušení zásad zpracování osobních údajů.

Rešerše je zaměřena na pracovněprávní oblast, je tedy věnována pozornost střetu zájmu zaměstnavatele a práva na soukromí zaměstnanců. Míra oprávněnosti monitoringu s ohledem na ochranu zaměstnance při plnění pracovních povinností a právo zaměstnavatele plnění těchto povinností kontrolovat.

Následuje vlastní práce, kde jsou syntézou propojeny získané informace z teoretické části práce. Poznatky jsou aplikovány na vybranou obchodní společnost, která je v úvodu nejdříve představena v anonymizované formě, vystupuje tedy jako společnost XX a. s. Samotná analýza se věnuje úkonům v pracovněprávním postupu dané společnosti při zpracování osobních údajů zaměstnanců, který se skládá z několika kroků a částí, stávající metody a procesy jsou analyzovány a identifikovány. Zkoumané jsou postupy probíhající před uzavřením pracovněprávního vztahu, dále v průběhu trvání zaměstnaneckého poměru, ale také i po jeho skončení. Dále je důkladně prozkoumána oblast soukromí zaměstnanců dané společnosti, jeho ochrana a způsoby a míra oprávněnosti monitoringu pracoviště a jednotlivých pracovníků. V této části je čerpáno z vnitropodnikových směrnic, řádů, a především hloubkových rozhovorů s odpovědnými osobami za danou oblast ve vybrané společnosti.

Závěrem jsou výsledky z vlastní práce komparovány s platnou legislativou a požadavky plynoucí z nařízení GDPR. To je základem pro návrhy opravných opatření či zlepšení již používaných postupů v analyzovaném podniku včetně vyhodnocení ekonomické náročnosti jejich realizace.

3 Literární rešerše

Jak uvádí Navrátil (2018), jsou osobní údaje a soukromí chráněny už po staletí, avšak s rozvojem společnosti a techniky stále více stoupá hodnota informací a s vývojem informačních technologií ochrana osobních údajů narůstá. Osobní údaje lze na jednu stranu využívat pro zákonem dovolené aktivity, ale na druhou stranu je lze snadno i zneužít.

Ochrana osobních údajů i soukromí se vyvíjí již dlouhou řadu let, i když z počátku ochrana soukromí neexistovala. Téměř všechny záležitosti se odehrávaly většinou veřejně. To se začalo postupně měnit s příchodem různých událostí, jako např. náboženské války, Velká francouzská revoluce, genocida. V době Velké francouzské revoluce vzniká i první psaný právní nástroj zabývající se ochranou soukromí – Deklarace práv člověka a občana z roku 1789. Na ni navázala Všeobecná deklarace lidských práv z roku 1948 a Mezinárodní pakt o občanských a politických právech (Navrátil, 2018).

Nový rozměr ochrany osobních údajů a soukromí přinesl rozvoj výpočetní techniky, robotizace. To sice přináší spoustu výhod, ale i mnoho hrozeb, jak zmiňuje Mates (2012).

Dle Navrátila (2018) byla prvním komplexním dokumentem, zabývajícím se ochranou osobních údajů na evropské úrovni, Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat z roku 2001. V České republice to byl zákon č. 101/2000 Sb., o ochraně osobních údajů, přijatý v roce 2000. Tento zákon byl do značné míry nahrazen Obecným nařízením o ochraně osobních údajů (GDPR) z roku 2016. Dne 24.4.2019 vešel v účinnost zákon č. 110/2019 Sb., o zpracování osobních údajů, jehož cílem je upřesnit práva a povinnosti vyplývající z Nařízení GDPR a zrušit dosud účinný zákon č. 101/2000 Sb., o ochraně osobních údajů (Chlebus, 2019).

3.1 Soukromí

Pojem soukromí je především v poslední době velmi diskutovaným tématem. Avšak tento pojem a právo na soukromí se objevuje už dávno v minulosti. Warren a Brandeis (1890) již v roce 1890 ve své práci definovali soukromí jako *„právo být ponechán o samotě (right to be alone)“*, a proto má pojem právo na soukromí kořeny ve Spojených státech amerických. Uvědomovali si, že každý člověk musí mít právo na ochranu své osoby a svého majetku.

S vývojem společnosti se vyvíjela i ochrana soukromí jedince. Např. Westin (1967) v 60. letech 19. st. vysvětloval soukromí jako právo člověka, instituce nebo skupiny rozhodnout se, jakým způsobem a do jaké míry budou informace o jeho osobě veřejné. Klíma (2002) poté uvedl, že každý má právo mít představu o svém vlastním soukromém životě. Podobný názor sdílí Kenyon (2006) – bere soukromí a jeho zveřejnění jako vlastní volbu každého člověka.

Navzdory tomu všemu se nepodařilo vytvořit jednotnou definici soukromí. I Mates (2006) uvádí, že ani judikatura Evropského soudu pro lidská práva nenavrhla závazné řešení. Pouze vyslovila názor, že každý má právo žít svůj život podle sebe a svých představ a nakládat se svým soukromím dle vlastního uvážení. To znamená, že soukromí je sice ochraňováno, avšak nelze najít tento pojem právně definovaný a každý si tento pojem vysvětluje a představuje jinak. Jedním z důvodu může být odlišnost různých kultur (Fialová, 2016).

Pohled na definici soukromí nabízí například Úřad pro ochranu osobních údajů: *„Soukromí můžeme stručně popsat jako osobní, intimní sféru člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského tvora. Pojem soukromí obsahuje rovněž hmotný i myšlenkový prostor jednotlivce, součástí soukromého života je i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.“* (ÚOOÚ, 2014)

Právo na soukromí zakotvuje Listina základních práv a svobod, a to především článek 7, který pojednává o nedotknutelnosti osoby a jejího soukromí. Dále článek 10, dle něj má každý člověk právo na soukromý a rodinný život a článek 13 zakazuje porušení listovního tajemství či jiných písemností a záznamů (LZPS, 1992).

Podle zákona č. 89/2012 Sb., občanský zákoník, je soukromí jedním ze základních osobnostních statků chráněných občanským právem a požívá zvláštní ochrany (§ 81 NOZ, 2012). Dále § 86 NOZ (2012) říká, že nikdo nesmí zasáhnout do soukromí jiného člověka, pokud k tomu nemá zákonný důvod.

3.2 Obecné nařízení o ochraně osobních údajů

Navrátil (2018) zmiňuje, že neopatrné užívání osobních údajů může vést k dalekosáhlým důsledkům. Z těchto důvodů se legislativa k ochraně osobních údajů neustále zdokonaluje a zpřísňuje. Na to navazuje Burian a Radičová (2016) a jako jeden z největších podnětů, na který musela Evropská unie reagovat, uvádí rozvoj nových technologií – internetové služby, elektronické obchodování a bankovnictví, využití sociálních sítí atd. Toto vše totiž s sebou přináší velký sběr a zpracování osobních údajů, monitorování a profilování fyzických osob, zaměstnanců, klientů. Rostoucí ochranu a zabezpečení nebylo již možné řešit novelami stávající směrnice č. 95/45/ES, proto vzniklo nové nařízení, které je nejúplnějším a nejbezprostřednějším opatřením k dispozici orgánům EU.

Nová právní úprava, a to Obecné nařízení o ochraně osobních údajů (GDPR), plným názvem nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů) ze dne 27. dubna 2016, představující právní rámec ochrany osobních údajů platný na celém území Evropské unie, stanovuje pravidla pro zpracování osobních údajů a práva subjektů údajů, hájí práva občanů proti neoprávněnému zacházení s jejich osobními údaji (Nezmar, 2017).

GDPR přebírá všechny dosavadní zásady ochrany a zpracování údajů. Platnosti nabyl 25. května 2018, v českém prostředí tak do značné míry nahradil zákon

č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (Nezmar, 2017). Některé záležitosti nejsou v GDPR upraveny, proto jsou například aspekty týkající se Úřadu pro ochranu osobních údajů a jiné dílčí záležitosti k dotvoření ochrany osobních údajů jako celku upravovány zákonem č. 110/2019 Sb., o zpracování osobních údajů. Případně umožňuje některé oblasti upravit na vnitrostátní úrovni, např. se jedná o zpracování osobních údajů pro účely výkonu svobody projevu, svobody vědeckého bádání a umělecké tvorby nebo práva na informace (Kenyon, 2006).

Navrátil (2018) ve své publikaci popisuje cíle GDPR, kterými je především přizpůsobení právního rámce ochrany osobních údajů dnešní době, sjednocení práva ochrany ve všech zemích, na které dopadá, posílení práv subjektů údajů, sjednocení výkladu GDPR dozorovými úřady a posílení důvěryhodnosti zemí Evropské unie.

Obecné nařízení přináší dva nové přístupy (Žůrek, 2017):

- princip odpovědnosti správce – stanovuje odpovědnost správce za dodržení povinností, ale také povinnost být schopen soulad doložit,
- přístup založený na riziku – správce musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a k tomu přizpůsobit i zabezpečení osobních údajů.

Dále GDPR přináší nová práva subjektu údajů:

Právo na výmaz – nenáleží-li správci žádný zákonný titul pro zpracování, je povinný na základě požadavku subjektu osobní údaje vymazat.

Právo na přenositelnost údajů – předání údajů jinému správci za určitých podmínek.

Právo vznést námitku – subjekt údajů má právo vznést námitku proti zpracování osobních údajů.

Právo na lidský zásah v případě rozhodnutí na bázi automatizovaného zpracování a profilování – subjekt údajů může vyjádřit svůj názor a napadnout rozhodnutí.

Nezmar (2017) říká, že GDPR přináší také nové povinnosti, např. povinnost vést záznamy o činnostech zpracování, posouzení vlivu na ochranu osobních údajů, předchozí konzultace, ohlašování ÚOOÚ, oznamování subjektu údajů případ porušení zabezpečení osobních údajů a ustanovení pověřence pro ochranu osobních údajů.

3.3 Osobní údaj

Osobním údajem je jakýkoli údaj, který se vztahuje k nějaké fyzické osobě a tato osoba je na jeho základě identifikovatelná. Dle Janečkové (2016) je vždy nutné se nejprve ujistit, že údaj, s nímž se pracuje, je údajem osobním ve smyslu zákona, pokud ano, zabývá se správce dalšími ustanoveními zákona.

Obecné nařízení o ochraně osobních údajů definuje v článku 4 osobní údaje jako: *„Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno,*

identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“

Za osobní údaje se považují údaje identifikační, které tvoří vztah mezi údaji a fyzickou osobou, a také další údaje, které jsou k identifikované osobě shromažďovány a zpracovávány. Fyzická osoba, které se osobní údaje týkají, je subjektem údajů (Žůrek, 2017).

Janečková (2016) uvádí speciální typy osobních údajů, a to:

- Citlivý údaj – údaje, které se fyzických osob týkají velmi blízce a jejichž zpracování může zasáhnout do soukromí člověka (národnostní, rasový nebo etnický původ, politický postoj, zdravotní stav atd.).
- Anonymní údaj – údaj, který nelze vztáhnout k určenému nebo určitelnému subjektu údajů.
- Zveřejněný osobní údaj – osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

3.3.1 Ochrana osobních údajů

Ochrana osobních údajů je základním právem fyzických osob zaručovaným Listinou základních práv Evropské unie i ústavami jednotlivých členských států EU (Navrátil, 2018).

Mates (2012) uvádí, že ochrana osobních údajů spadá do okruhu práv na ochranu soukromí, který tvoří široká škála vzájemně souvisejících práv, funkcí je chránit osobnost člověka jako celku.

V případě porušení práv v důsledku zpracování osobních údajů v rozporu s GDPR má subjekt údajů právo na soudní ochranu. Dotčený má právo podat stížnost u dozorového úřadu v členském státě svého bydliště, v místě výkonu zaměstnání nebo tam, kde došlo k porušení ochrany práv (Navrátil, 2018).

3.3.2 Zpracování osobních údajů

Zpracováním osobních údajů definované v čl. 4 odst. 2 Obecného nařízení je myšlena jakákoliv operace, kterou správce nebo zpracovatel provádí systematicky s osobními údaji, automatizovaně nebo jinými prostředky.
Žůrek (2017) zmiňuje, že se musí jednat o „kvalifikované“ nakládání s osobními údaji, zpracováním osobních údajů není každá činnost či nakládání s osobními údaji. Správce provádí činnost s osobními údaji systematicky za určitým účelem a z určitého pohledu.

GDPR zdůrazňuje, že zpracování osobních údajů musí být prováděno zákonným, spravedlivým způsobem a musí být transparentní. Osobní údaje by měly být shromažďovány v přiměřeném množství, relevantní a v řádu nezbytnosti, dále by měly být uloženy po nezbytnou dobu a zpracovány pouze v případě neschopnosti

dosáhnout účelu jinými prostředky. Osobní údaje by měly být zpracovány způsobem, který zaručí bezpečnost a důvěrnost těchto údajů, mimo jiné k zabránění neoprávněnému přístupu k těmto údajům (Navrátil, 2018).

Jak již bylo zmíněno, je zpracování osobních údajů prováděno pomocí automatizovaných postupů, jako je shromáždění (postup s cílem získat osobní údaje za účelem jejich uložení a zpracování), uchovávání (udržování osobních údajů v podobě vhodné pro jejich zpracování), blokování (omezení způsobů či prostředků zpracování osobních údajů, s výjimkou nezbytných zásahů), výmaz nebo zničení (ukončení zpracování osobních údajů), zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, pozměnění, vyhledání, nahlédnutí, použití a další (Janečková, 2016).

3.3.3 Zásady zpracování osobních údajů

Žůrek (2017) označuje zásady zpracování osobních údajů za základní stavební kameny ochrany osobních údajů, je na nich postaveno celé Obecné nařízení. Zásady jsou zevšeobecněným vyjádřením dílčích povinností. Správce má odpovědnost za jejich dodržení a musí být schopen soulad doložit, což je nepřetržitým, komplexním procesem.

Základní zásady zpracování osobních údajů upravuje článek 5 Obecného nařízení. Nulíček (2017) poznamenává, že jsou to základní pravidla, od kterých se odvíjí všechny procesy zpracování a určují to, jak může správce s osobními údaji nakládat.

Zásada zákonnosti je jedna z nejdůležitějších principů, jelikož vyjadřuje, že zpracování musí probíhat v souladu s právními předpisy. To znamená, že správce může osobní údaje zpracovávat pouze v případě, má-li k tomu minimálně jeden právní důvod (Žůrek, 2017). Navrátil (2018) doplňuje, že aby bylo zpracování osobních údajů v souladu se zákonem, musí se dít buď na základě souhlasu dotčené osoby, nebo na základě jiného, přímo stanoveného důvodu. Navíc musí být zpracování provedeno takovým způsobem, aby bylo pro dotčené osoby předvídatelné, nesmí být protiprávní, to znamená, že nesmí probíhat za nelegálním či nelegitimním účelem a nesmí být v rozporu s právním řádem obecně (Nulíček, 2017).

Zásada korektnosti a transparentnosti říká, že správce nesmí vůči subjektu zastírat účel zpracování osobních údajů, dále by měl být subjekt informován o tom, kdo, jakým způsobem a v jakém rozsahu osobní údaje zpracovává a komu jsou osobní údaje předávány (Žůrek, 2017). Navrátil (2018) uvádí, že u zásady korektnosti by měla odpovědná osoba zohledňovat zájmy a očekávání dotčených osob, nesmí je bezdůvodně přehlížet nebo zneužívat jejich mylných představ. V zásadě transparentnosti jde především o to, že by dotčené osoby měly mít právo rozhodnout o tom, které – v rámci zákonem daných hranic – údaje o sobě poskytnou. K porušení těchto zásad nejčastěji dochází nesprávným či nedostatečným splněním informační povinnosti (Nulíček, 2017).

Zásada účelového omezení vyjadřuje, jak může správce s osobními údaji nakládat, vymezením účelu si správce určí, z jakého důvodu osobní údaje zpracovává. Účel musí být určitý, výslovně vyjádřený a legitimní (Pattynová, 2018). Osobní údaje nesmějí být zpracovávány způsobem, který je s účelem neslučitelný. Od účelu zpracování se odvíjí právní důvod zpracování osobních údajů a další povinnosti, proto

je specifikace účelu podstatná (Žůrek, 2017). Nulíček (2017) doplňuje, že účel může vyplývat přímo ze zákona, pokud tomu tak není, musí dojít ke stanovení účelu nejpozději při sběru dat.

Zásada minimalizace údajů zdůrazňuje, že je možné shromažďovat a zpracovávat pouze ty osobní údaje, které jsou přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu (Pattynová, 2018). To brání správci požadovat po subjektu údajů více informací, než je potřeba. Tato zásada je do jisté míry i bezpečnostním prvkem, neboť čím méně osobních údajů je zpracováno, tím hrozí subjektu menší riziko úniku či zneužití těchto údajů, poznamenává Žůrek (2017).

Zásada přesnosti říká, že zpracované údaje musí být přesné, musí odpovídat skutečnosti a v případě potřeby být aktualizované. Aktualizaci údajů je povinen správce provádět za účelem zajištění přesnosti (Žůrek, 2017). V případě nepřesnosti musí správce přijmout opatření k tomu, aby nepřesné údaje opravil nebo zlikvidoval, uvádí Nuklíček (2017). Dále zmiňuje, že přesnost údajů neznamená jejich pravdivost, pokud subjekt údajů poskytne údaje nepřesné, správce za jejich nepřesnost neodpovídá. To doplňuje Navrátil (2018), který uvádí, že v případě zjištění nepřesnosti musí být údaje okamžitě vymazány či opraveny. Opravu či aktualizace údajů musí správce provést také na základě žádosti subjektu údajů (Nulíček, 2017).

Zásada omezení uložení vyjadřuje povinnost uchovávat osobní údaje po dobu nezbytnou pro účely zpracování (Nulíček, 2017). Je to z toho důvodu, že zpracování osobních údajů zasahuje do soukromí fyzické osoby a může představovat určité bezpečnostní riziko, vysvětluje zásadu omezení Žůrek (2017). Subjekt údajů by měl být informován o době, po kterou budou jeho osobní údaje zpracovávány, doba může být stanovena i relativně (ve vztahu k určité rozhodné události). Avšak může to být i před tím, než určená doba uplyne, a to v případě, kdy pomine účel zpracování, v tom případě Obecné nařízení ukládá povinnost správci takové osobní údaje vymazat (Navrátil, 2018).

Zásada integrity a důvěrnosti ukládá povinnost zpracovat osobní údaje takovým způsobem, aby bylo zajištěno zabezpečení před neoprávněným či protiprávním zpracováním, před náhodnou ztrátou, zničením či poškozením (Nulíček, 2017). K zabezpečení dochází prostřednictvím vhodných technických nebo organizačních opatření, k čemuž patří i zajištění toho, že neoprávněné osoby nebudou mít k datům přístup ani nebudou mít přístroje ke zpracování dat (Navrátil, 2018).

Zásada odpovědnosti je chápána jako zajištění dodržování zásad stanovených Obecným nařízením a povinnost správce toto dodržování doložit (Pattynová, 2018). Navrátil (2018) uvádí, že tímto správce neodpovídá pouze za výsledek, ale také za postupy a musí přijímat opatření k zabránění porušení GDPR. Opatření jsou kontrolována dozorovými úřady.

3.4 Subjekt údajů

Subjektem údajů je fyzická osoba, které se osobní údaje týkají. Osobní údaje se vztahují vždy jen k fyzické osobě, nikoli k osobě právnické. Osoba musí být určená nebo

alespoň určitelná. Dále Nezmar (2017) upozorňuje, že osobní údaje se týkají žijící osoby, Obecné nařízení vylučuje svoji působnost na údaje zemřelých osob.

3.5 Správce a zpracovatel

Správcem je subjekt, jakékoliv právní formy, určující účel a prostředky zpracování osobních údajů a který za zpracování odpovídá. Údaje zpracovává pro účely, jež vyplývají z jeho činnosti či pro vlastní účely. Správcem může být i fyzická osoba, jejíž činnost naplňuje znaky zpracování, a pokud nepůjde o výjimky (Nezmar, 2017). Navrátil (2018) upozorňuje, že správce musí zavést vhodná technická a organizační opatření, kterými zajistí a doloží zpracování osobních údajů dle GDPR.

Zpracovatele si najímá správce, aby pro něj zpracoval osobní údaje. Jak Žůrek (2017) podotýká, správce může, ale nemusí, zpracovatele využít, ale přizvat si ho může kdykoliv bez souhlasu subjektu údajů. Zpracovatel může provádět pouze takové operace, kterými je od správce pověřen a je zpracovatelem ve vztahu k osobním údajům poskytnutým správcem. Nezmar (2017) také uvádí, že stejně jako u správce není rozhodná právní forma zpracovatele.

Jak uvádí Žůrek (2017), je správce i zpracovatel povinen spolupracovat na požádání s dozorovým úřadem při plnění jeho úkolů.

3.6 Úřad pro ochranu osobních údajů

Součástí ochrany osobních údajů jsou v jednotlivých členských státech EU dozorové úřady, kterým jsou svěřeny úkoly a pro jejich plnění pravomoci (Žůrek, 2017).

Úřad pro ochranu osobních údajů (ÚOOÚ) je nezávislý veřejný orgán, který dohlíží na uplatňování právních předpisů související s ochranou údajů díky svým vyšetřovacím a nápravným pravomocím. Úřad poskytuje odborné poradenství, monitoruje uplatňování Obecného nařízení s cílem chránit základní práva a svobody fyzických osob, vyřizuje podané stížnosti kvůli porušení GDPR (Evropská komise, 2018). Navrátil (2018) doplňuje, že úřad by měl také zvyšovat povědomí veřejnosti o rizicích, pravidlech, zárukách a právech týkajících se zpracování osobních údajů.

Každý členský stát má takový svůj úřad, jednotlivé úřady mezi sebou spolupracují tak, aby bylo Obecné nařízení uplatňováno jednotně. Hlavním kontaktním místem pro otázky týkající se ochrany osobních údajů je úřad v tom státě, kde má osoba trvalé bydliště, případně společnost své sídlo. Avšak jak poznamenává Evropská komise (2018), pokud zpracovává společnost údaje v jiných členských státech EU, může být hlavní kontaktní místo v jiném členském státě. Každý dozorový úřad je příslušný k plnění úkolů a výkonů pravomocí svěřených Obecným nařízením na území svého státu a základním předpokladem dozorového úřadu je jeho nezávislost při plnění úkolů a výkonů pravomocí dle GDPR (Žůrek, 2017).

V České republice plní roli dozorového úřadu Úřad pro ochranu osobních údajů, který byl založen v červnu 2000 jako nezávislý správní orgán v oblasti ochrany osobních údajů. Jak zmiňuje Žůrek (2017), zůstalo zřízení, kvalifikace a podmínky způsobilosti pro členy atd. v kompetenci zákona o zpracování osobních

údajů. V § 54 odst. 2 zákona o zpracování osobních údajů je vymezení činností Úřadu následující:

a) *„provádí dozor nad dodržováním povinností stanovených zákonem při zpracování osobních údajů,*
b) *ověřuje zákonnost zpracování osobních údajů na podnět subjektu údajů podle § 31,*
c) *přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování osobních údajů a informuje o jejich vyřízení,*
d) *projednává přestupky a ukládá pokuty,*
e) *poskytuje konzultace v oblasti ochrany osobních údajů,*
f) *informuje veřejnost o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním osobních údajů,*
g) *informuje správce a zpracovatele o jejich povinnostech v oblasti ochrany osobních údajů a*
h) *vykonává další působnost stanovenou mu zákonem".*

3.7 Sankce a pokuty

V zájmu zajištění ochrany osobních údajů je součástí GDPR systém sankcí, které mohou být uloženy dozorovým úřadem v případě porušení některé z povinností stanovených v Obecném nařízení. Sankční část má preventivní a donucující účinek na adresáty právní normy (Nulíček, 2017). Nezmar (2017) doplňuje, že ukládání správních pokut musí být účinné, přiměřené, ale zároveň odrazující.

Dle směrnice 95/46/ES bylo každému státu ponecháno právo určit vhodná opatření k řádnému plnění směrnice. Z toho důvodu se právní úprava sankcí poměrně lišila. Obecné nařízení tak správní sankce sjednotilo. Určuje vhodná opatření k dodržování GDPR, ale členské státy mohou stanovit další nepřiznivé následky za porušení (Nulíček, 2017).

Navrátil (2018) uvádí, že GDPR vychází z principu, že za jakékoliv porušení by měly být uloženy sankce včetně správních pokut. Nezmar (2017) toto doplňuje a říká, že za každé porušení Obecného nařízení nemusí být udělena pokuta, ale správce může být například nejprve upozorněn na porušující operace, může mu být uděleno napomenutí či nařízení uvést zpracování do souladu.

Dozorový úřad rozhoduje o uložení správní pokuty, je na něm, zda uloží sankci či jiné opatření. Při ukládání správní pokuty a určování její výše zohlední úřad konkrétní případ, jedná se o princip individualizace správních pokut (Nulíček, 2017). Pattynová (2018) uvádí konkrétní případy, které se zohledňují při ukládání správní pokuty:

- povaha, závažnost a délka trvání porušení,
- rozsah a účel zpracování,
- počet poškozených a míra způsobené škody,
- zavinění,
- zmírňování škod,
- odpovědnost,

- předchozí porušení,
- spolupráce s dozorovým úřadem,
- kategorie osobních údajů,
- hlášení incidentů,
- splnění nařízených opatření,
- dodržování schváleného kodexu chování nebo mechanismu pro vydávání osvědčení,
- jakékoliv jiné přitěžující nebo polehčující okolnosti.

GDPR rozděluje pokuty dle závažnosti do dvou kategorií. Za méně závažná porušení lze uložit pokutu dle odst. 4 článku 83 Obecného nařízení až ve výši 10 000 000 EUR, v případě podniku až ve výši 2 % celkového ročního obratu za předchozí finanční rok. Jedná se například o porušení ustanovení týkající se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů aj. V případě vážnějších porušení hrozí uložení správní pokuty až do výše 20 000 000 EUR, v případě podniku až 4 % celkového ročního obratu, uvedeno v odst. 5 článku 83 Obecného nařízení. Do této kategorie spadá např. porušení povinností upravující zásady a zákonnost zpracování, podmínky souhlasu se zpracováním osobních údajů, podmínky zpracování zvláštních kategorií osobních údajů a práva subjektu údajů (Nezmar, 2017).

3.8 Ochrana osobních údajů na pracovišti

Jak uvádí Mates (2012), dochází v průběhu pracovněprávního vztahu ke zpracování mnoha osobních údajů, a to již od začátku, to znamená ve chvíli, kdy se potenciální zaměstnanec přihlásí do výběrového řízení.

Základní vztah mezi fyzickou osobou (subjektem údajů) a zaměstnavatelem (správcem údajů) upravuje z hlediska pracovního práva zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a zákon č. 262/2006 Sb., zákoník práce (Bartík, 2016).

Nové Obecné nařízení o ochraně osobních údajů zasahuje také do personalistiky. Nařízení se snaží nalézt rovnováhu mezi potřebou informací zaměstnavatele a právem žadatele o práci na respektování soukromého života. Dále vyžaduje od zaměstnavatele otevřenost k žadatelům (Nezmar, 2017).

3.8.1 Osobní údaje před vznikem pracovního poměru

Do této fáze patří jakýkoliv kontakt zájemce o zaměstnání a zaměstnavatele před uzavřením pracovní smlouvy. Tento kontakt většinou začíná reakcí zájemce na zveřejněnou nabídku práce.

Během výběrového řízení zaměstnavatel již shromažďuje velké množství údajů o uchazečích. Dle § 30 odst. 2 zákoníku práce, ve znění pozdějších předpisů smí zaměstnavatel vyžadovat od fyzické osoby ucházející se u něj o práci takové informace, které bezprostředně souvisejí s uzavřením pracovní smlouvy. To znamená, že kromě identifikačních údajů potencionálního zaměstnance lze vyžadovat i jiné informace, např. osvědčení o určitém vzdělání, potvrzení o zaměstnání aj.

Zákon o zaměstnanosti stanovuje údaje, které není přípustné ve fázi výběru zaměstnanců zjišťovat. V § 12 odst. 2 ZoZ jsou stanoveny informace, které nesmí zaměstnavatel při výběru zaměstnanců vyžadovat, jedná se o tzv. citlivé údaje (národnost, rasový či etnický původ, politické postoje, náboženství, sexuální orientace atd.). Na žádost uchazeče o zaměstnání je zaměstnavatel povinen prokázat potřebu osobního údaje (Mates, 2012).

Při osobním kontaktu zaměstnavatele s potenciálním zaměstnancem může docházet k diskriminačnímu jednání, jak zmiňuje Mates (2012), v praxi se tak často bohužel stává. Zaměstnavatelé nejprve prověřují, zda uchazeč splňuje potřebné požadavky (získané vzdělání, praxe atd.), při pohovoru se poté často zaměstnavatelé dotazují na informace, které zákon o zaměstnanosti zakazuje, nejčastěji se vyskytují otázky týkající se budoucího mateřství, počtu dětí a zajištění jejich péče. Uchazeč má právo poskytnutí těchto informací odmítnout.

Dále Bartík (2016) upozorňuje, že získané a zpracovávané údaje musí zaměstnavatel chránit před zneužitím a použít je jen k takovému účelu, ke kterému byly shromážděny, a to jen po nezbytně nutnou dobu. To tedy znamená, že v okamžiku výběru vhodného uchazeče neexistuje již důvod zpracovávat údaje ostatních uchazečů a končí tak oprávnění s těmito údaji dále nakládat.

Nezmar (2017) doplňuje, že úkolem zaměstnavatele je zajistit, aby osoby podílející se na náboru a výběru zaměstnanců, věděly, že platí pravidla ochrany osobních údajů a že s nimi musí zacházet dle požadavků GDPR. Dále uvádí, že získané údaje je možné využít pouze pro konkrétní výběrové řízení a nesmí jich shromažďovat více, než k výběru skutečně potřebuje. Zaměstnavatel by se také neměl snažit získat takové údaje, které ve finále potřebuje pouze od osoby, kterou se rozhodl přijmout, od všech uchazečů o zaměstnání. V případě ověření poskytnutých informací o osobě je nutné, aby o tom daná osoba věděla a bylo jí jasné, jakým způsobem k ověření dojde. Po skončení výběrového řízení by měl zaměstnavatel zaslané životopisy neúspěšných uchazečů zlikvidovat. Toto doplňuje Janečková (2018), která říká, že pokud si chce zaměstnavatel pro potřeby dalšího využití životopisy ponechat, může tak učinit pouze se souhlasem dotčených osob, kterým musí být znám účel a doba nového využití.

Janečková (2018) také vysvětluje, proč pro zpracování osobních údajů uchazečů o zaměstnání není potřeba souhlas uchazečů, uvádí: *„bez souhlasu je totiž možné údaje zpracovávat pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů“*. Zaměstnavatel dává veřejným sdělením najevo, že hledá nové pracovní síly, zveřejňovány bývají většinou základní požadavky na pracovní místo, požadován bývá strukturovaný životopis a sdělení kvalifikačních předpokladů a je ponecháno na uchazeči, jaké údaje o sobě v požadovaných dokumentech skutečně uvede. Jelikož je naplněna podmínka dle článku 6 odst. 1 písm. b) GDPR, není třeba, aby zaměstnavatel údaje zpracovával s „formalizovaným“ souhlasem uchazečů. Avšak uchazečům musí být znám účel i rozsah poskytnutí osobních údajů, na základě toho je poskytují sami o své vůli.

3.8.2 Osobní údaje během trvání pracovního poměru

Po skončení výběrového řízení je s vybraným uchazečem uzavřena pracovní smlouva a dochází k navýšení množství zpracovávaných osobních údajů nově přijatého zaměstnance. Obvykle bývá zakládán osobní spis zaměstnance, který je charakterizován jako soubor zcela nebo částečně standardizovaných dokumentů odpovídající právním předpisům a zaznamenávající průběh a výsledky jednotlivých personálních činností (Bartík, 2012). Paragraf 312 zákoníku práce uvádí, že osobní spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v pracovněprávním vztahu. Spis obsahuje např. osobní dotazník, profesní životopis, doklady o dosaženém vzdělání, potvrzení o předchozím zaměstnání, lékařský posudek atd.

Nelze pořizovat kopie dokladů (např. rodného listu), a to ani se souhlasem subjektu údajů. Tyto doklady totiž mohou obsahovat další údaje včetně údajů třetích osob, které nejsou pro zaměstnavatele nezbytné. Do osobního spisu lze uložit jen ty kopie dokladů, které obsahují pouze osobní údaje nezbytné pro zaměstnavatele nebo se souhlasem zaměstnance, zmiňuje Janečková (2018).

Mates (2012) uvádí, že osobní údaje zaměstnance lze rozdělit do tří skupin:

1. Do této skupiny patří údaje, které zaměstnavatel potřebuje k plnění svých zákonných povinností, a je tedy oprávněn je vyžadovat. Jedná se o jméno a příjmení, trvalé bydliště, datum narození, rodné číslo, dosažené vzdělání atd.
2. Další skupinou jsou údaje potřebné pro určitý účel, o kterém je třeba zaměstnance informovat a nakládat s nimi pouze v rámci tohoto účelu. Řadí se sem číslo bankovního účtu, číslo občanského průkazu, osobní údaje rodinných příslušníků.
3. Poslední skupinou jsou dobrovolně poskytnuté údaje zaměstnavateli zaměstnancem, např. číslo soukromého mobilního telefonu.

Pracovní vztahy jsou založeny na pracovní smlouvě mezi zaměstnavatelem a zaměstnancem, pro splnění povinností dle smlouvy musí zaměstnavatel zpracovávat osobní údaje, bez tohoto zpracování by nebylo možné smlouvu plnit. Proto k činnostem vedoucím k plnění smlouvy a k vedení záznamů o průběhu zaměstnání není třeba souhlasu pracovníků. Zaměstnanci by ale měli vědět, jak bude organizace jejich záznamy používat (Janečková, 2018).

Nezmar (2017) zmiňuje, že by organizace měla kontrolovat, jaké záznamy jsou o zaměstnancích uchovávány a ujistit se, že neuchovává informace, které jsou irelevantní, přílišného rozsahu nebo zastaralé. Následně vymazat informace bez skutečného významu nebo bez zákonné povinnosti je držet. Dále v případě zveřejňování informací o zaměstnanci (např. daňové správě) je nutné zveřejnit pouze informace nezbytně nutné. V případě nutnosti zveřejnit osobní údaje bez souhlasu či oprávnění zaměstnance lze v některých případech s odvoláním na výjimku stanovenou v GDPR, to může nastat při trestním stíhání, při vyšetřování ohledně daňových povinností či soudním řízení. Nezmar (2017) také apeluje na to, že je nutné uchovávat záznamy o zaměstnancích v bezpečí, ať už se jedná o papírové či digitální dokumenty.

Dle ÚOOÚ (2013) má právo zaměstnavatel zpracovávat tyto osobní údaje:

- *„pro evidenční listy důchodového pojištění zasílaných na OSSZ (datum a místo narození, rodné příjmení, rodné číslo, trvalé bydliště atd.)*
- *pro správný výpočet mzdy (vzdělání, praxe)*
- *pro správný výpočet měsíčních záloh na daně (druh pobíraného důchodu)*
- *pro zjištění přesného data nároku na odchod do starobního důchodu (počet dětí – u žen)*
- *pro plnění povinného podílu osob se zdravotním postižením na celkovém počtu zaměstnanců (zdravotní znevýhodnění)*
- *pro placení zdravotního pojištění (zdravotní pojišťovna)*
- *za účelem hlášení zaměstnávání cizinců (státní občanství)*
- *prohlášení poplatníka daně z příjmu*
  - *pokud zaměstnanec uplatňuje daňové zvýhodnění a manželka je zaměstnána (jméno, příjmení manželky, název, adresa zaměstnavatele)*
  - *pokud zaměstnanec uplatňuje zvýhodnění na vyživované dítě (jméno, příjmení a rodné číslo dítěte)"*.

3.8.3 Osobní údaje po ukončení pracovního poměru

I po ukončení pracovního poměru vznikají další dokumenty zařazené do osobního spisu zaměstnance, poznamenává Mates (2012), jedná se například o doklad o skončení pracovního poměru, kopie pracovního posudku, doklad o vypořádání vzájemných pohledávek, kopie vydaného potvrzení o zaměstnání atd.

Na základě dvou zákonných důvodů – plnění právní povinnosti a oprávněných zájmů správce může zaměstnavatel zpracovávat osobní údaje bývalého zaměstnance i po ukončení pracovního poměru (Janečková, 2018).

První důvod rozvádí Janečková (2018) tak, že po skončení pracovního poměru je možno osobní údaje uchovávat jen z důvodů, které jsou stanovené v právním předpise. Jedním z právních předpisů je například zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ten říká, jak dlouho jsou zaměstnavatelé povinni uchovávat stejnopisy evidenčních listů, záznamy o skutečnostech vedených v evidenci, mzdové listy, účetní záznamy atd.

Stanoveny jsou tedy druhy dokumentů, které musí být uchovány a také doba, po kterou je nezbytné osobní údaje bývalých zaměstnanců uchovávat. Mezi uchovávané dokumenty nepatří např. životopis nebo různá osvědčení, která po skončení pracovního poměru ztratila relevanci. Takové dokumenty by měly být zaměstnanci vráceny nebo prokazatelně zlikvidovány (Bartík, 2016). Nezmar (2017) doplňuje, že ostatní dokumenty mají být bezpečně zlikvidovány po vypršení povinnosti organizace záznamy uchovávat.

K uchování některých dokumentů z důvodu oprávněných zájmů správce dochází z vlastního zájmu, a to například v případě, pokud by hrozil soudní spor týkající se zaniklého pracovního poměru. Může tak činit po dobu obecné promlčecí doby, která je dle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tříletá (Janečková, 2018).

3.9 Práva a povinnosti zúčastněných stran

Role v problematice ochrany osobních údajů jsou v pracovněprávních vztazích rozděleny poměrně jednoznačně. Zaměstnavatel vystupuje jako správce osobních údajů a zaměstnanec jako subjekt údajů.

3.9.1 Práva zaměstnavatele

Práva zaměstnavatele se opírají především o § 316 odst. 1 zákoníku práce. Zaměstnavatel má právo požadovat po zaměstnanci efektivní práci a zároveň chránit svou podnikatelskou činnost před nebezpečím, jako je způsobená škoda či trestná činnost. Dále může zaměstnavatel po zaměstnanci vyžadovat, aby neužíval výrobní a pracovní prostředky pro vlastní potřebu (§ 316, odst. 1 ZP). Zaměstnavatel může tuto skutečnost přiměřeným způsobem kontrolovat (Vidrna, Koudelka, 2013).

Zaměstnavatel, jako správce osobních údajů, má oprávnění osobní údaje zpracovávat, nezbytným předpokladem jsou právní důvody zpracování. Zpracování osobních údajů se vždy váže k účelu, na základě kterého se určí právní důvod zpracování (ÚOOÚ, 2017). Dle článku 6, odst. 1 Obecného nařízení patří mezi právní důvody:

- *„subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,*
- *zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,*
- *zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,*
- *zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,*
- *zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,*
- *zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů zejména pokud je subjektem údajů dítě*“.

3.9.2 Práva zaměstnance

Práva zaměstnance jako subjektu údajů tvoří důležitou část ochrany osobních údajů, jelikož vyvažují vztah mezi správcem a subjektem údajů, který může být v některých případech nerovný z toho důvodu, že subjekt údajů musí často zpracování osobních údajů strpět (Žůrek, 2017).

Zaměstnanci mají zákonné právo být informováni, že osobní údaje týkající se jejich osoby jsou shromažďovány, používány, konzultovány nebo jinak zpracová-

vány, také v jakém rozsahu a k jakému účelu jsou zpracovávány (Nulíček, 2017). Nezmar (2017) zmiňuje, že zaměstnanec má právo na přístup k informacím, pokud o to zaměstnavatele požádá.

Dle článku 15 GDPR má zaměstnanec právo na přístup k osobním údajům, to znamená, že může po zaměstnavateli požadovat informaci, zda zpracovává osobní údaje, které se ho týkají. Také má právo získat kopii zpracovávaných osobních údajů (Janečková, 2018).

Zaměstnanec má dále právo požadovat opravu nepřesných osobních údajů (článek 16 GDPR) a právo na výmaz osobních údajů, které se ho týkají, pokud existuje důvod uvedený v odst. 1 článku 17 GDPR. Dále může pracující požádat nadřízeného o omezení zpracování osobních údajů, jsou-li splněny podmínky v odst. 1 článku 18 GDPR a dle článku 20 GDPR mu mohou být poskytnuty údaje o jeho osobě, které může předat jinému správci.

Zaměstnanec má právo vznést námitku proti zpracování jeho osobních údajů a může okomentovat nebo podat námitku proti sledování nebo monitorování jeho činnosti na pracovišti, uvádí Nezmar (2017).

Jedním z posledních práv je, že zaměstnanec má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování (článek 22 GDPR).

Žůrek (2017) upozorňuje, že zajištění řádného výkonu práv subjektu údajů je nezbytnou podmínkou pro soulad zpracování jako celku s Obecným nařízením a porušení práv subjektu Obecné nařízení „trestá“ jednou z vyšších sazeb.

3.9.3 Povinnosti zaměstnavatele

Jednou z prvních povinností je stanovit účel, proč a k jakému cíli se osobní údaje shromažďují a následně zpracovávají. Tato povinnost je jednou z nejzákladnějších a nejdůležitějších povinností zaměstnavatele jako správce, uvádí Janečková (2016). Dále by měl správce před zahájením zpracování stanovit prostředky zpracování a stanovit způsob zpracování osobních údajů. Zpracovávány by měly být pouze přesné osobní údaje odpovídající stanovenému účelu v nejnutnějším rozsahu. Správce má také povinnost uchovávat nashromážděné osobní údaje po nezbytnou dobu, jakmile pomine účel, je správce povinen provést výmaz osobních údajů (článek 25 GDPR).

Článek 12 Obecného nařízení uvádí základní povinnost správce přijmout vhodná opatření k poskytnutí veškerých informací subjektům údajů *„stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků“*.

Zaměstnavatel musí zabezpečit osobní údaje svých zaměstnanců před protiprávním zpracováním, náhodnou ztrátou, zničením nebo poškozením (Janečková, 2018). Nulíček (2017) zmiňuje, že zaměstnavatel by měl být schopen doložit soulad zpracování údajů s GDPR nejlépe pomocí vedené dokumentace. Záznamy o činnostech zpracování by měly obsahovat informace uvedené v článku 30 Obecného nařízení.

Zaměstnavatel jako správce má obecnou povinnost spolupracovat s dozorovým úřadem při plnění jeho úkolů dle článku 31 Obecného nařízení. Články 33 a 34 Obecného nařízení přináší povinnost ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu.

3.9.4 Povinnosti zaměstnance

Mates (2012) upozorňuje, že v rámci pracovněprávního vztahu musí dodržovat povinnosti v rámci GDPR i zaměstnanec, který zpracovává osobní údaje na základě smlouvy se správcem údajů. Osobní údaje může zpracovávat za daným účelem a v rozsahu stanoveném správcem. Správce musí pověřeným osobám určit podmínky zpracování a měly by být začleněny do jejich pracovní náplně či přeneseny do interního výkonu řízení.

Dle § 47 zákona č. 110/2019 Sb., o zpracování osobních údajů jsou zaměstnanci správce údajů přicházející do styku s osobními údaji u správce povinni zachovávat mlčenlivost o osobních údajích a o organizačních a technických opatřeních, jejichž zveřejnění by ohrozilo bezpečnost osobních údajů. Tato povinnost trvá i po ukončení zaměstnání či příslušné práce.

3.10 Monitoring zaměstnanců

Jednou z oblastí, která je v důsledku rozvoje odposlouchávacích, kamerových a jiných podobných zařízení stále častěji veřejností vnímána, je také ochrana soukromí zaměstnance při výkonu práce pro zaměstnavatele, zmiňuje Bartík (2016). Za poslední desítky let došlo ke značnému rozvoji informační a komunikační technologie, a to včetně jejich dostupnosti. To dává možnost zaměstnavateli sledovat elektronickou poštu zaměstnance, jeho činnost na internetu, telefonní hovory a monitorovat jeho činnost kamerami. Pokrok v komunikačních a informačních technologiích představuje nová rizika pro ochranu lidských práv a svobod. Díky novým technologiím jsou v určitých případech stírány rozdíly mezi pracovním a soukromým životem, např. práce z domu či být dosažitelný na telefonu.

Na pracovišti může docházet ke střetu zájmů zaměstnavatele a zaměstnance. Na jedné straně vystupuje zaměstnanec s povinností řádně plnit své pracovní povinnosti v určené době a s využitím pracovních prostředků jemu přidělených. Na druhé straně je zaměstnavatel, který má právo plnění těchto povinností kontrolovat. Mates (2012) uvádí, že zaměstnanci jsou přesvědčeni o nároku na soukromí na pracovišti a často jsou pobouřeni jejich sledováním. Zaměstnavatel tento nárok nepopírá, ale zastává názor, že právo na soukromí zaměstnance musí být v práci přizpůsobeno, a to z toho důvodu, že zaměstnanec se u zaměstnavatele zdržuje pouze kvůli výkonu práce, za kterou je ohodnocen.

Zákoník práce dovoluje zaměstnavateli přiměřeně kontrolovat zaměstnance, který nesmí využívat výrobní a pracovní prostředky pro svou osobní potřebu. Ale nesmí bez závažného důvodu narušovat soukromí zaměstnance. Existuje-li důvod k zavedení kontrolních mechanismů, je povinností zaměstnavatele informovat o rozsahu a způsobu kontroly (§ 316 zákoníku práce).

3.10.1 Kamerové systémy

Kamerové systémy se staly běžnou součástí našeho života a člověk se s nimi může setkat na různých místech. V dnešní době je to pravděpodobně jeden z nejrozšířenějších způsobů sledování osob. I když jsou tyto systémy podporovány veřejností, mají zásadní vliv na život běžných lidí a vzniká tak nutnost ochrany osobních údajů a soukromí, podotýká Nezmar (2017).

Kamerové systémy jsou instalovány za různými účely, jako je např. ochrana jedinců, ochrana majetku, veřejný pořádek, boj s kriminalitou, odhalování trestné činnosti. Kamery se začaly postupně objevovat i na pracovištích, zaměstnavatelé je užívají především z těchto důvodů (Bartík, 2016):

- ke sledování, zda zaměstnanci plní své pracovní povinnosti a nejsou porušovány zákazy,
- k ochraně majetku.

Jelikož prostřednictvím kamerového systému zpravidla dochází i ke zpracování osobních údajů, je nutné dodržovat pravidla stanovené Obecným nařízením. Správce provozující kamerový systém odpovídá za zpracování, které jeho prostřednictvím provádí (Žůrek, 2017). Nezmar (2017) doplňuje, že GDPR chápe použití kamerových systémů jako sběr osobních dat, pokud na záznamech lze rozpoznat tváře jednotlivých osob. Jelikož je v dnešní době kvalita kamer vysoká, týká se to téměř každého, kdo vlastní kamerové zabezpečení. Proto se instalací kamer stává organizace správcem osobních údajů a měla by být schopna odůvodnit tento sběr a zpracování údajů.

Stanovisko k provozování kamerového systému vydal i ÚOOÚ. Uvádí, že za zpracování osobních údajů je považováno provozování kamerového systému pouze v případě, je-li prováděn záznam pořizovaných záběrů nebo je účelem kamer identifikace fyzických osob. Údaje jsou tedy osobními za předpokladu, že na jejich základě lze identifikovat konkrétní fyzickou osobu. Fyzická osoba je identifikovatelná, pokud jsou ze záznamu patrné její charakteristické rozpoznávací znaky (ÚOOÚ, 2018).

Pro zpracovávání osobních údajů získaných prostřednictvím kamerového systému musí být právní důvod. Žůrek (2017) uvažuje dva právní důvody. První z nich je důvod dle čl. 6 odst. 1 písm. c) GDPR, splnění právních povinností správce. Za druhé je to důvod nezbytnosti zpracování pro účely oprávněných zájmů příslušného správce či třetí strany dle čl. 6 odst. 1 písm. f) GDPR.

Zaměstnanec musí být řádně informován o tom, že je jeho pracovní prostor monitorován. Tento monitorovaný prostor by měl být označen piktogramem kamery s uvedením správce, aby subjekt údajů věděl, na koho se v případě otázek či uplatnění práv obrátit (Žůrek, 2017). Zaměstnavatel nesmí využívat monitorování zaměstnanců bez omezení, kamery nesmí být umístěny do míst zaručující určité soukromí např. v šatnách, sociálních zařízení atd. (Mates, 2012).

3.10.2 Přístup na internet a e-mailová pošta zaměstnanců

Vývoj výpočetní techniky ulehčil a zrychlil mnoha zaměstnancům jejich práci, proto v dnešní době nalezneme na většiny pracovišť počítače, které jsou svěřeny zaměstnancům k jejich pracovnímu výkonu. Dá se tedy předpokládat, že zaměstnavatelé chtějí, aby byla poskytnutá technika využita pouze k plnění pracovních úkolů. Jak již bylo řečeno, § 316 odst. 1 ZP uvádí, že zaměstnanci nesmí výpočetní techniku využívat k osobní potřebě a zaměstnavatel to může přiměřeným způsobem kontrolovat.

Na počítačích mají zaměstnanci většinou přístup k internetu. Zaměstnavatel by měl v pracovním řádě jasně vymezit, jak mohou zaměstnanci s internetem během pracovní doby zacházet, zda ho mohou využívat pro osobní účely a případně v jaké míře. Dále může zaměstnavatel využívání internetu pro osobní účely omezit tím, že blokuje internetové stránky, které nejsou potřebné pro pracovní výkon (Morávek, 2013).

Pokud je zaměstnancova aktivita na internetu sledována, měl by k tomu být, jak uvádí § 316 ZP, důvod a zaměstnanec by měl být o možnosti sledování informován. Při sledování aktivity na internetu dochází ke zpracování osobních údajů, jehož právním důvodem jsou oprávněné zájmy zaměstnavatele dle čl. 6 odst. 1 písm. f) Obecného nařízení. Sbírání informací o zaměstnancem navštěvovaných internetových stránkách je zásahem do soukromí, ale zaměstnavatel může tento typ kontroly vykonávat, pokud je účelem zjistit, zda zaměstnanec navštěvuje internetové stránky nesouvisející s výkonem jeho práce (Škubal, 2012).

Zaměstnanci využívají počítače také k e-mailové korespondenci. Morávek (2013) upozorňuje, že pokud zaměstnavatel výslovně nesvolí, nesmí zaměstnanec na firemním počítači řešit soukromé e-maily, každý e-mail, který dorazí na pracoviště, je tedy považován za pracovní, pokud není důvod se domnívat jinak.

Zaměstnavatel nemá právo sledovat, monitorovat nebo zpracovávat obsah korespondence svých zaměstnanců. Může pouze sledovat počet e-mailů došlých a odeslaných, hlavičku a předmět e-mailu a požadovat po zaměstnancích, aby své soukromé záležitosti v pracovní době a na pracovišti nevyřizovali. Zaměstnavatel by měl o svém záměru sledovat počet odeslaných a přijatých e-mailů zaměstnance informovat, a to nejlépe hned při navazování pracovního poměru (Bartík, 2016).

3.10.3 Služební telefony

Další oblastí, kde se zaměstnavatelé snaží kontrolovat své zaměstnance, je používání služebních telefonů. Může se jednat o pevné linky i o mobilní telefony, v současné době pevné linky ustupují do pozadí a k pracovním účelům se využívají spíše mobilní telefony, které zaměstnavatelé svým zaměstnancům často poskytují jako tzv. služební mobilní telefony.

Dle § 316 ZP by zaměstnanci měli využívat služební mobilní telefony pouze k výkonu pracovní náplně a nepoužívat je k soukromým záležitostem, pokud zaměstnavatel nestanoví jinak. Zaměstnavatel může kontrolovat, zda jsou uskutečňované hovory pouze pracovní, ale nesmí být kontrolován obsah hovorů a nesmí být pořizovány jejich záznamy. Může zaznamenávat telefonní čísla, na která bylo ze slu-

žebního telefonu voláno, a u zaměstnance si ověřit, zda se jedná o soukromý či pracovní hovor. Pokud zaměstnavatel vede záznamy o tom, kolik daný zaměstnanec učiní soukromých hovorů, jejich délku a volaná čísla, jedná se již o zpracování osobních údajů (Bartík, 2016).

3.10.4 Služební automobily

Dalším prostředkem, který zaměstnavatel zaměstnanci může svěřit, je služební automobil. Náklady na provoz jsou poměrně vysoké, proto samozřejmě existuje i zde snaha kontrolovat zaměstnance, zda automobil nevyužívá k osobní potřebě, jako je uvedeno v § 316 ZP. Monitorování většinou probíhá na základě technologie GPS, která určuje přesnou polohu vozidla, a i zpětně lze prohlédnout celou trasu jízdy. Zaměstnavatel toto zařízení může používat, stejně jako v předchozích případech, za účelem ochrany majetku a dodržování pracovněprávních předpisů (Bartík, 2016).

V případě zavedení GPS musí zaměstnavatel počítat s požadavky na ochranu osobních údajů. Mezi možné právní důvody zpracování tohoto typu osobních údajů je dle čl. 6 odst. 1 písm. f) Obecného nařízení, ochrana oprávněných zájmů správce údajů. Případně se může jednat i o souhlas zaměstnance dle čl. 6 odst. 1 písm. a) Obecného nařízení. Tento případ může nastat v situaci, kdy je povoleno využívat vozidlo i k soukromým účelům a zaměstnanec souhlasí se zapnutou GPS (Žůrek, 2017).

4 Vlastní práce

4.1 Představení společnosti

Společnost XX a. s. je bankovní společností působící jako univerzální banka v České republice. Dle CZ-NACE, 2018 je obor společnosti Peněžnictví a pojišťovnictví (Ostatní peněžní zprostředkování) – *„tato třída zahrnuje přijímání vkladů nebo náhrad podobných vkladům a zvětšování úvěrových a půjčkových fondů, poskytování úvěrů může mít různé formy a tyto činnosti jsou obecně vykonávány finančními institucemi, jinými než centrálními bankami".*

Společnost XX a. s. poskytuje své služby všem klientským segmentům, tzn. fyzickým osobám, malým a středním podnikům, korporátním a institucionálním klientům. Svým zákazníkům nabízí širokou škálu bankovních produktů a služeb, včetně produktů a služeb ostatních společností skupiny. Produktové portfolio celé skupiny je tedy následující:

- standardní bankovní služby,
- financování potřeb spojených s bydlením,
- pojistné produkty,
- penzijní fondy,
- produkty kolektivního financování a správa aktiv,
- specializované služby (leasing a factoring),
- služby spojené s obchodováním s akciemi na finančních trzích.

Banka byla založena v minulém století jako banka pro poskytování služeb v oblasti financování zahraničního obchodu a volnoměnových operací s působností na československém trhu, může se tedy opírat o historickou a stabilní základnu.

XX a. s. se řadí mezi velké podniky, působí po celé České republice, centrála je v Praze, ale pobočky a útvary jsou ve větších i menších městech. Společnost zaměstnává zaměstnance na hlavní pracovní poměr, dále ve společnosti působí osoby na základě dohody o provedení práce či dohody o provedení činnosti a dále osoby na stáži či praxi.

Firma má jeden útvar Personalistika a mzdy, který se stará o zaměstnance celé banky, každý zaměstnanec má přiděleného svého konkrétního personalistu, který uchovává potřebné dokumenty a na kterého se může zaměstnanec v případě potřeby obrátit. Minimálně v každém kraji je specialista útvaru Náboru, který má na starost nábor zaměstnanců v dané lokalitě.

4.2 Zpracování osobních údajů ve společnosti XX a. s.

Vzhledem k tomu, že zaměstnanci jsou přijímáni za výkonem pracovní činnosti u společnosti XX a. s., dochází ke zpracování jejich osobních údajů. Společnost vystupuje jako správce osobních údajů a jednotliví zaměstnanci jako subjekty osobních údajů. Správce osobních údajů zodpovídá za to, že s osobními údaji bude zacházeno řádně, v souladu s právními předpisy a nedojde k jejich zneužití. Při zpracování

osobních údajů se společnost řídí právními předpisy, zejména Obecným nařízením o ochraně osobních údajů, zákonem o zpracování osobních údajů, zákoníkem práce, zákony upravující povinnost mlčenlivosti (např. občanským zákoníkem, zákonem o bankách či zákonem o pojišťovnictví) a zákonem o některých službách informační společnosti, který upravuje zasílání nevyžádaných obchodních sdělení.

Ve společnosti platí přísná pravidla stanovující, který zaměstnanec či útvar může mít přístup k osobním údajům a jaké osobní údaje může zpracovávat. Společnost využívá interní předpisy, kde je zmíněná legislativa aplikována na potřeby daného podniku. Má ustanoveny předpisy jako např. Pravidla pro ochranu osobních údajů, Povinnosti vyplývající z GDPR, Ochrana osobních údajů při používání bezpečnostních kamerových systémů a další. Předpisy slouží především ke stanovení zásad zpracování osobních údajů a seznamují s postupy a úkoly zaměstnance, kteří nakládají s osobními údaji. Další předpisy seznamují s náborem, výběrem a přijímáním zaměstnanců, odměňováním zaměstnanců, vznikem, změnou a ukončením pracovněprávního vztahu atd. K dispozici je také praktický průvodce pro nového zaměstnance a dokument s informacemi o zpracování osobních údajů, který zaměstnance seznamuje se zpracováním jeho osobních údajů.

XX a. s. se také zavazuje, že nepředá osobní údaje mimo společnost, s výjimkou případů, kdy má zaměstnancův souhlas nebo k tomu opravňuje právní předpis. Firma se snaží předcházet únikům dat důsledným řízením přístupu k důvěrným informacím a kanálům, kterými by mohly informace firmu opustit. Pro zajištění správného zacházení s informacemi jsou veškeré zvlášť důvěrné dokumenty viditelně i elektronicky označeny. Jsou používány technické nástroje, které detekují neautorizovaný přístup k datům nebo jejich odeslání mimo společnost. Cílem společnosti je mít nastavené procedury takovým způsobem, aby bylo možné reagovat na případné incidenty a včas zajistit nápravu.

Každý zaměstnanec má právo na přístup ke svým údajům, na vysvětlení, přenos údajů, i další práva, pokud se domnívá, že zpracování není v pořádku. V případě potřeby či nejasností mohou zaměstnanci kontaktovat HR linku, obrátit se mohou také na stanoveného pověřence pro ochranu osobních údajů nebo v případě problému podat stížnost k dozorovému úřadu.

Společnost ve svém interním předpise uvádí, že shromažďuje a zpracovává pouze takové údaje, aby mohla řádně fungovat jako zaměstnavatel. Zpracovává údaje z těchto kategorií:

- základní údaje zaměstnance – identifikační údaje, soukromé kontaktní údaje, základní údaje o zaměstnání, údaje o benefitech, údaje nezbytné pro plnění povinností v oblasti daní, zdravotního a sociálního pojištění, životního a penzijního připojištění, biometrické údaje, informace o bezúhonnosti, informace o záznamech v insolvenčním rejstříku,
- základní HR údaje – finanční údaje, údaje o dostupnosti, zdravotní údaje,
- rozšířené HR údaje – hodnocení, cíle, talentové údaje, údaje o vzdělávání,

- fyzické, technické a komunikační údaje – údaje o spolupráci, pracovní kontaktní údaje, technický profil, fyzický profil, komunikace a interakce, záznamy interakce s klienty,
- údaje o kontrole – údaje o vnitřní kontrole, rizikové údaje.

Ke zpracování osobních dat ve společnosti dochází v důsledku sledování legitimního účelu. Účely plynou z toho, že firma musí dodržovat zákonné a smluvní povinnosti, především jako zaměstnavatel. Proto se zpracovávají data např. za účelem základní pracovněprávní agendy, zpracování mezd, evidence dovolených, organizace práce, bezpečnosti marketingu, benefitů pro zaměstnance. V rámci společnosti platí určitá etická pravidla uvedená v Etickém kodexu, v těchto případech se zpracovávají informace za účelem kontroly dodržování těchto pravidel a předcházení případných nesrovnalostí.

Společnost dále uvádí, že osobní údaje získává na základě dobrovolného rozhodnutí zaměstnance. Osobní údaje jsou požadovány z důvodu plnění pracovněprávních nebo smluvních povinností, případně pro fungování firmy, pro zpracování údajů tedy svědčí oprávněný zájem. Není tedy nutný souhlas zaměstnance ke zpracování údajů, ten totiž vychází z podepsání pracovní smlouvy. Bez zpracování údajů by nebylo možné splnit uzavřenou smlouvu a řádně fungovat, a proto společnost považuje předání údajů za povinné.

Data týkající se osobních údajů v listinné podobě ukládá společnost XX a. s. v uzamykatelných skříních v kancelářích útvaru Personalistika a mzdy a mají k nim přístup pouze pracovníci tohoto útvaru. Není dovoleno nahlížet do spisů nepovoleným osobám. Pro elektronické zpracování osobních údajů je důležité zabezpečení informačního systému, což má na starost IT oddělení. Ochrana je také zvýšena přístupovými oprávněními, které má jen omezený počet osob, pouze ti, kteří s údaji pracují. Ochrana je také podpořena povinností mlčenlivosti, která se vztahuje na zaměstnance zpracovávající údaje.

Zaměstnancům útvarů Personalistika a mzdy jsou k dispozici vnitřní předpisy upravující problematiku ochrany osobních údajů, kde mají stanoveno, jak postupovat a zacházet s údaji. Bohužel bylo zjištěno, že zaměstnanci nepodstupují pravidelná školení, kde by byli seznamováni se změnami v této oblasti.

4.3 Zpracování osobních údajů před uzavřením pracovního poměru

Do této etapy se řadí výběr uchazečů o zaměstnání na pozici vypsanou společností. Právní předpisy nestanovují přesnou formu ani způsob výběrového řízení při výběru nových zaměstnanců. Je tedy na společnosti, aby si celý proces náboru potenciálních zaměstnanců zvolila sama, to potvrzuje i odst. 1 § 30 ZP: *„Výběr fyzických osob ucházejících se o zaměstnání z hlediska kvalifikace, nezbytných požadavků nebo zvláštních schopností je v působnosti zaměstnavatele, nevyplývá-li ze zvláštního právního předpisu jiný postup.“*.

4.3.1 Přihlášení uchazeče do výběrového řízení

Pokud společnost XX a. s. identifikuje volnou pozici, manažer požádá o otevření nové pozice, je-li pozice otevřená dochází k předvýběru kandidátů, dále následují pohovory, vybranému vhodnému kandidátovi je nabídnut nástup na pracovní pozici a v případě přijetí kandidátem musí být nástup administrován.

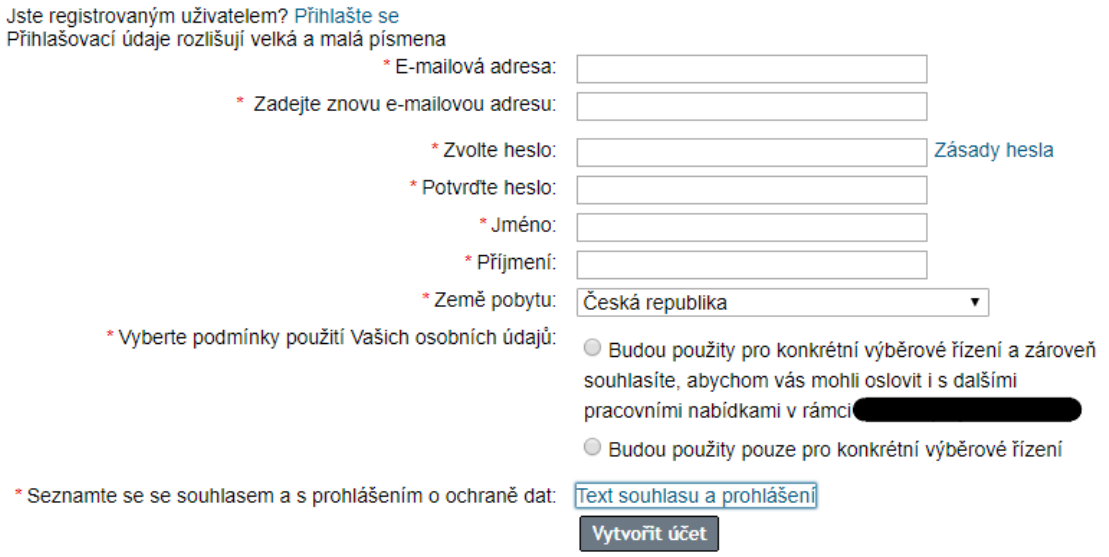
Kandidáty pro výběr na vypsanou pozici zajišťuje specialista náboru (případně personální agentura). Povinností specialisty náboru, příp. HR Business partnera, je nahlášení volného pracovního místa na úřad práce minimálně 30 dní předem. Veřejnost je dále informována o nově vypsaných pozicích inzerováním na webových stránkách společnosti XX a. s. nebo na specializovaných inzertních serverech, inzercí na vysokých školách, veletrzích pracovních příležitostí a pomocí propagace na sociálních sítích (např. LinkedIN, jobs.cz). K využití personálních agentur dochází pouze v omezené míře, zejména v případech, kdy se nalezení vhodného kandidáta ze standardních zdrojů jeví jako málo pravděpodobné, případně pokud bylo dosavadní vyhledávání neúspěšné.

Společnost XX a. s. se řídí platnými právními předpisy, proto po uchazečích požaduje pouze údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy. Každý kandidát v případě zájmu o pracovní pozici musí předložit motivační dopis a strukturovaný životopis. Společnost kandidáty ubezpečuje, že zaslané materiály považuje za diskrétní.

Uchazeč o zaměstnání má možnost přihlásit se do výběrového řízení pomocí registrace do databáze společnosti přes webové stránky. Musí vyplnit základní údaje o své osobě a zaškrtnout jednu ze dvou podmínek použití jeho osobních údajů. První z nich říká, že údaje uchazeče budou využity pouze pro konkrétní výběrové řízení. V druhé stojí, že údaje budou využity v konkrétním výběrovém řízení a zároveň společnost může uchazeče oslovit i s dalšími pracovními nabídkami. V případě výběru druhé možnosti je souhlas platný po dobu 2 let (od skončení daného výběrového řízení). Souhlas může uchazeč kdykoli odvolat.

Zájemci o práci, kteří se přihlašují do výběrového řízení, by měli odsouhlasit, že se seznámili s prohlášením o ochraně soukromých dat, které je k dispozici při registraci do databáze společnosti. Společnost uchazeče informuje o účelu zpracování jejich osobních údajů – údaje jsou zpracovávány za účelem výběrových řízení na volná pracovní místa, aby společnost mohla s uchazeči jednat a posoudit možnosti uplatnění. Za účelem průběhu výběrového řízení na volnou pracovní pozici jsou zpracovávány údaje:

- identifikační údaje (jméno, příjmení, akademické tituly, adresa trvalého bydliště, datum a místo narození, osobní fotografie atd.),
- profilové údaje uchazeče (životopis a údaje v něm obsažené),
- soukromé kontaktní údaje uchazeče (doručovací adresa, e-mail, telefonní číslo).



Obr. 1 Registrace uchazečů o zaměstnání do databáze společnosti XX a. s.
Zdroj: interní

4.3.2 Výběrové řízení

Výběrové řízení je proces, během kterého kompetentní osoby, za použití metod výběru, vybírají kandidáta, který nejlépe ze všech splňuje předpoklady pro výkon poptávaných činností. Všechna výběrová řízení mají ve společnosti XX a. s. obdobnou podobu, co se formy a stylu týká. Avšak u jednotlivých pracovních pozic jsou odchylky závisející na náplni pracovní činnosti dané pozice. Společným rysem je informační povinnost zaměstnavatele, za prvé seznámit uchazeče s ochranou jeho osobních dat a za druhé s právy a povinnostmi vyplývajícími z uzavření pracovní smlouvy. Zaměstnavatel je dále při výběru nového zaměstnance povinen rovně zacházet se všemi uchazeči, přistupovat stejně k zaměstnání žen a mužů a respektovat zákaz přímé či nepřímé diskriminace (věk, pohlaví, etnický původ, sexuální orientace atd.).

Inzeráty na volné pozice jsou obvykle zveřejňovány zhruba po dobu dvou týdnů. Následně jsou zaslané životopisy vyhodnoceny a vyhovující uchazeči jsou nejčastěji telefonicky kontaktováni členem útvaru Náboru a pozváni na osobní pohovor a jsou jim sděleny informace o čase a místě výběrového řízení. Kontaktováni jsou i neúspěšní uchazeči, většinou pomocí e-mailu jim je poděkováno za zájem o pozici a vysvětlen důvod odmítnutí.

Rozlišuje se výběr zaměstnance z vnitřních nebo vnějších zdrojů, kdy je přednostně prováděn výběr vhodného kandidáta z vnitřních zdrojů. Výběr kandidátů na vypsanou pozici provádí příslušný odpovědný vedoucí zaměstnanec ve spolupráci s členy útvaru Nábor a ve své kompetenci na základě posouzení žádostí předem vybraných kandidátů, individuálních přijímacích pohovorů s kandidáty a jejich vyhodnocení. Výběrová řízení mohou trvat různě dlouho dobu, mohou být i víceko-

lová, to platí především u vyšších pozic. Přesné způsoby výběru nového zaměstnance si určuje vedoucí daného oddělení. Metody výběru zaměstnanců se ve společnosti XX a. s. rozlišují na standardní a specifické. Do standardních metod patří:

- **přijímací pohovor**, který probíhá za přítomnosti vedoucího zaměstnance,
- k **ověřování referencí** dochází před finálním rozhodnutím, především pokud uchazeč pracoval či pracuje ve finančních institucích. S poskytnutím referencí musí kandidát souhlasit a potvrdit svůj souhlas podepsáním standardního formuláře,
- **testy odborných znalostí** nejsou povinnou součástí výběrového řízení, jejich použití navrhuje odpovědný vedoucí zaměstnanec a rovněž odpovídá za sestavení testů,
- **Assessement Centrum** se používá jako výběrová metoda pro obchodní pozice a manažerské pozice.

Mezi specifické metody výběrového řízení se řadí:

- **psychodiagnostické metody** jsou volitelnou součástí všech výběrových řízení, avšak pro manažerské pozice jsou povinné. Při výběru a využití psychodiagnostických metod se vždy vychází s požadovaných předpokladů pro úspěšný výkon příslušné pracovní pozice (osobní vlastnosti a schopnosti vhodné pro danou pozici),
- **personální agentury** lze využít v případě, že se nalezení vhodného kandidáta ze standardních zdrojů jeví jako málo pravděpodobné, případně pokud bylo dosavadní vyhledávání neúspěšné.

Společnost má dále sestavenou příručku k pohovoru, kde jsou například k dispozici tipy na vedení interview či diskriminační otázky. Ve výběrovém řízení by měl odpovědný zaměstnanec řídící pohovor po uchazeči požadovat představení, nechat si vysvětlit informace uvedené v životopise, zmapovat potřebné dovednosti a schopnosti kandidáta, zajímat se o výkon, zaměřit se na motivaci a ambice, zjistit připravenost uchazeče, prověřit stresovou odolnost a zmapovat schopnost sebereflexe. Společnost XX a. s. dbá na to, aby otázky bezprostředně souvisely s uzavřením pracovní smlouvy, vzděláním a prací samotnou. Dále uvádí, že mezi otázky považované za diskriminující patří například otázky týkající se soukromí, národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženského vyznání, filozofického přesvědčení, sexuální orientace či zdravotního stavu. Kandidát se s podezřením na diskriminaci může obrátit na Státní úřad inspekce práce a zaměstnavateli by mohla být uložena pokuta za porušení zákazu diskriminace či nerovného zacházení.

Ve chvíli, kdy je zvolen vhodný uchazeč, je tento uchazeč telefonicky kontaktován, jsou mu nabídnuty přesné podmínky nástupu a pokud uchazeč přijímá, je výběrové řízení ukončeno. Po ukončení výběrového řízení společnost informuje neúspěšné uchazeče pomocí telefonického či e-mailového kontaktu, pokud tito kandidáti zvolili možnost, aby jejich údaje byly použity i pro další výběrové řízení, je připojena informace, že jejich osobní údaje poslouží k dalšímu zpracování a pokud s tím nesouhlasí, tak ať kontaktují personální oddělení firmy, které jejích údaje zlikviduje.

Veškeré dokumenty o kandidátech (písemné, elektronické) vzniklé v souvislosti s výběrovým řízením jsou archivovány a skartovány podle vnitřního předpisu společnosti Spisová služba a archivace, resp. po dobu platnosti souhlasu externího kandidáta s uchováním a zpracováváním osobních údajů.

4.4 Zpracování osobních údajů během trvání pracovního poměru

Po dobu pracovního poměru jsou zaměstnavatelem zpracovávány osobní údaje ve velkém množství. Po ukončení výběrového řízení společnosti XX a. s. nejčastěji člen útvaru Náboru kontaktuje telefonicky vybraného uchazeče a informuje ho o přijetí, dále ho seznámí s právy a povinnostmi vyplývajícími z pracovní smlouvy a také s pracovními podmínkami a podmínkami odměňování. Tímto krokem se předchází situaci, kdy zaměstnanec uzavře smlouvu, aniž by byl dostatečně obeznámen se všemi úkony s ní spojenými. Následně je uchazeči poskytnut prostor pro rozhodnutí přijetí pracovní nabídky.

Pokud uchazeč pracovní nabídku přijme, musí předložit základní doklady nutné pro vznik pracovního poměru:

- vyplněný osobní dotazník,
- čestné prohlášení uchazeče o uzavření pracovněprávního vztahu,
- výpis z rejstříku trestů,
- doklad o nejvyšším dosaženém vzdělání,
- barevnou fotografii,
- povolení k zaměstnání a povolení k pobytu, jedná-li se o cizího státního příslušníka, který nemá na území ČR trvalý pobyt, s výjimkou osob s trvalým pobytem ve státech EU.

Dále musí nejpozději do osmi dnů po nástupu odevzdat potvrzení o zaměstnání (zápočtový list) od předchozího zaměstnavatele, případně potvrzení z Úřadu práce o ukončení evidence (jestliže tam byl veden). Nový zaměstnanec musí absolvovat povinnou zdravotní prohlídku a doložit lékařský posudek. Od lékaře je zpracovávána pouze informace, zda, případně v jakém rozsahu, je zaměstnanec způsobilý k práci. Personalista zabezpečí převzetí všech dokumentů od nového zaměstnance, provede věcnou kontrolu originálů dokumentů a jejich fotokopii a vrátí neprodleně originály dokumentů zpět. Personalista dále zajistí předání základních informací novým zaměstnancům prostřednictvím pověřených zaměstnanců, jedná se zejména o seznámení s Pracovním řádem společnosti, Kolektivní smlouvou, Pravidly pro používání komunikačních prostředků, Etickým kodexem zaměstnanců, Informací o zpracování osobních údajů pro zaměstnance a další spolupracující osoby.

Zaměstnanec se dále musí zúčastnit vstupního školení, které se koná vždy k prvnímu pracovnímu dni v měsíci na centrále v Praze pro všechny nově nastupující zaměstnance v rámci celé ČR. Zde jsou s novými zaměstnanci podepsány dvě vyhotovení pracovní smlouvy a další dokumenty, jako například mzdový výměr, dohoda o srážkách (např. při využití pevné telefonní linky pro soukromé účely).

Odpovědný vedoucí nového zaměstnance vyplní elektronický nástupní list a postoupí ho HR Business partnerovi tak, aby nejpozději deset pracovních dnů přede dnem nástupu budoucího zaměstnance byl schválený v útvaru Personalistika a mzdy. Vedoucí dále zaměstnance seznámí v rámci svých pracovních povinností a v rozsahu potřebném pro konkrétní pracoviště a pracovní pozici zaměstnance s Organizačním řádem, Stanovami společnosti, Předpisy a zajištění BOZP a požární ochrany, Ochranou bankovního tajemství a osobních údajů, Povinností zachovávat mlčenlivost.

4.4.1 Osobní dotazník zaměstnance

Každý nový zaměstnanec ještě před podepsáním pracovní smlouvy musí vyplnit osobní dotazník, který je zaměstnanci zaslán nejčastěji pomocí e-mailu a zaměstnanec jej zašle elektronicky vyplněný zpět příslušnému personalistovi. Osobní dotazník si společnost XX a. s. sestavila sama dle vlastních potřeb.

Osobní dotazník společnosti XX a. s. obsahuje základní osobní údaje zaměstnance, jako jsou jméno a příjmení. Dále rodné číslo, datum a místo narození, zdravotní pojišťovna, což je například využíváno pro plnění povinností sociálního a zdravotního zabezpečení. Dále jsou vyžadovány informace o adrese trvalého bydliště a adrese doručovací, telefonické spojení, informace o nejvyšším dosaženém vzdělání a posledním zaměstnání. Zaměstnanec také uvádí svůj rodinný stav a v případě, že má děti, vyplňuje zde i jejich jméno, příjmení a datum narození, pro účely výpočtu daňové povinnosti. Zaměstnanec dále zaznamenává, zda má čistý trestní rejstřík a zda byl evidován na Úřadu práce.

Společnost XX a. s. v osobním dotazníku nepožaduje po zaměstnanci vyplnit žádné citlivé údaje.

4.4.2 Pracovní smlouva

V odst. 1 § 33 ZP je řečeno, že pracovní poměr se zakládá pracovní smlouvou mezi zaměstnavatelem a zaměstnancem. Jak je uvedeno v odst. 2 § 34 ZP musí být pracovní smlouva uzavřena písemně a dle odst. 1 musí obsahovat:

a) druh práce, který má zaměstnanec pro zaměstnavatele vykonávat,
b) místo nebo místa výkonu práce, ve kterých má být práce podle písmene a) vykonávána,
c) den nástupu do práce.

Každá ze smluvních stran musí obdržet jedno vyhotovení smlouvy (odst. 5 § 34 ZP).

V hlavičce pracovní smlouvy společnosti XX a. s. je uvedeno, kdo za zaměstnavatele smlouvu se zaměstnancem uzavírá a dále jméno, datum narození a trvalé bydliště zaměstnance. Pracovní smlouva ve společnosti XX a. s. obsahuje zákonné povinnosti, tzn. druh práce, místo výkonu práce a den nástupu. Dále je zde uvedena délka zkušební doby a zda je smlouva uzavřena na dobu určitou či neurčitou, v případě doby určité je uvedeno, do jakého data je pracovní poměr sjednán. Na výši měsíční mzdy je odkázáno do mzdového výměru, to platí i o srážkách ze mzdy, které jsou ujednány v dohodě o srážkách. Pracovní smlouva také informuje a právech a povinnostech zaměstnance i zaměstnavatele.

4.4.3 Osobní spis zaměstnance

Personalista společnosti XX a. s. při uzavření pracovního poměru založí osobní spis zaměstnance a odpovídá i následně za řádné vedení osobního spisu, tj. za aktuální věcný obsah i časový sled. Personalista také zabezpečí ochranu osobních údajů zaměstnance a s osobním spisem nakládá podle označeného stupně důvěrnosti.

Do osobního spisu je umožněno nahlížet zaměstnanci, kterého se týká, odpovědnému zaměstnanci útvaru Personalistika a mzdy, přímému odpovědnému vedoucímu zaměstnanci daného zaměstnance, zaměstnanci útvaru Vnitřní audit a útvaru Compliance na základě pověření k provedení kontroly, orgánu státní správy kompetentního k nahlédnutí do osobního spisu na základě pověření k provedené kontrole. Personalista poskytuje informace o zaměstnanci jen s jeho souhlasem, pokud příslušný obecně právní předpis vztahující se k poskytnutí informace nestanoví jinak.

Obsah osobního spisu tvoří:

- Pracovní smlouva a její změny / originál
- Mzdový výměr nebo Manažerská smlouva / originál
- Čestné prohlášení uchazeče o uzavření pracovněprávního vztahu ke společnosti/ originál
- Prohlášení zaměstnance při nástupu do společnosti XX a. s. / originál
- Nástupní list
- Potvrzení o zdravotní způsobilosti k práci (lékařská prohlídka) / originál
- Doklad o nejvyšším dosaženém vzdělání / kopie
- Rozhodnutí o invaliditě, případně doklad o zdravotním znevýhodnění / kopie
- Osobní dotazník / originál

Společnost nezařazuje do osobního spisu kopii občanského průkazu. Občanský průkaz požaduje pouze k nahlédnutí pro ověření uvedených údajů v osobním dotazníku. Zaměstnanec jej předkládá při podpisu pracovní smlouvy a do osobního dotazníku je zaznamenáno číslo dokladu, datum ověření a kdo tento doklad ověřil plus jeho podpis.

Zaměstnanec je povinen hlásit nejpozději do osmi pracovních dnů veškeré změny svých osobních údajů útvaru Personalistika a mzdy, a to buď formou informačního systému či pomocí formuláře Hlášení změn útvaru Řízení lidských zdrojů.

4.4.4 Informační systém

V dnešní době se pro zpracování osobních údajů zaměstnanců v hojném počtu využívají informační systémy, které zjednodušují práci personálního oddělení. Společnost XX a. s. využívá program SAP, což je podnikový informační systém, pomocí kterého je možné sledovat procesy probíhající ve firmě ve společném prostředí a pomáhá zjednodušit běžný provoz firmy (sap.com, 2019).

V SAPu společnost uchovává dokumenty v elektronické podobě, první informace o zaměstnanci jsou do systému přepsány z osobního dotazníku a postupně jsou doplňovány další údaje.

Do personálního informačního systému mají přístup zaměstnanci útvaru Personalistika a mzdy a HR. Dále každý zaměstnanec, který zde může sledovat všechny informace o své osobě. Tento systém není webový, proto lze navštěvovat pouze skrz softwarového klienta a díky tomu je chráněn proti útokům na osobní údaje zaměstnanců zvenčí. Informační systém je také chráněn heslem, který si zvolí každý zaměstnanec sám a musí jej každé dva měsíce obměňovat.

Součástí SAP portálu je karta zaměstnance a každý zaměstnanec může takto nahlédnout na údaje o své osobě. V kartě zaměstnance najdeme organizační data – pozice, organizační jednotka, přidělený personalista, HR Business Partner atd. Dále základní data k osobě (jméno, příjmení, rodné číslo, rodinný stav), kontakty (adresa, e-mail), informace k pracovní angažovanosti a mzdě, bankovní spojení, daňová data (daňové slevy, zvýhodnění), zdravotní pojišťovna, nejvyšší dosažené vzdělání. Některé z údajů si zaměstnanec může upravit sám, např. základní údaje o své osobě či zdravotní pojišťovnu, dosažené vzdělání. Ostatní upravuje personální referent.

V systému má dále zaměstnanec k dispozici výplatní pásky, informace ke svým pracovním cestám, přehled ročního zúčtování daně. Také je zde evidována docházka a řádná dovolená. V rámci systému funguje aplikace pro řízení vzdělávání, Portál SAP HR, což je nástroj, který každému zaměstnanci umožní aktivní řízení svého vzdělávání, například plnění povinných elektronických školení, přihlašování do externích kurzů, volbu termínu. Pro zaměstnance je zde připravena také HR Linka, kde jsou k dispozici různé informace, návody, žádosti, formuláře, předpisy a online konzultace.

Každý zaměstnanec by při opuštění pracovního místa měl uzamknout svůj počítač, aby zamezil přístupu nepovolaným osobám. Heslo, které do systému používá by mělo být dostatečně bezpečné a nemělo by být nikomu sdělováno. Veškeré informace, které jsou důvěrné a přísně důvěrné, by měly být označeny a v případě zasílání externím příjemcům šifrovány.

4.4.5 Identifikační karta

Identifikační karta ve společnosti XX a. s. plní funkci zaměstnaneckého průkazu, další funkce má podle technologické vybavenosti objektu, ve kterém držitel ID karty vykonává pracovní působnost. Dostane ji každý zaměstnanec při nástupu do zaměstnání, její převzetí musí potvrdit podpisem. Karta je označována jménem, příjmením, přiděleným osobním číslem a fotografií zaměstnance. Na kartě je také uveden název společnosti, proto v případě ztráty je nutné, co nejdříve tuto ztrátu nahlásit, aby mohla být zablokována a nedošlo tak k jejímu zneužití.

Identifikační karta slouží především ke vstupu na pracoviště, a to do budovy samotné, jednotlivého patra a případně místnosti. Jelikož má společnost několik budov po celé ČR, je zaměstnanci umožněn pouze vstup přímo do budovy jeho pracoviště a daného patra, příp. místnosti a do budovy centrály (avšak ne do všech pater

a místností). Ke každé kartě je možné nastavit vstupní práva individuálně, záleží na pracovní pozici.

Karta dále slouží téměř na všech pracovištích pro tisk z tiskárny, kdy po odeslání dokumentů z počítače je nutné se pomocí karty přihlásit k tiskárně a až poté zvolit, co přesně má být vytisknuto. Také je užívána pro služební osobní motorová vozidla a vjezd do parkingu společnosti.

Při ukončení pracovního poměru se zaměstnancem odpovědný vedoucí tento odchod nahlásí útvaru Personalistika a mzdy, karta je zablokována a zaměstnanec ji musí v poslední pracovní den odevzdat. Karta musí být archivována po dobu 10 let od ukončení pracovního poměru a poté zlikvidována.

4.4.6 Fotografie

Fotografie je po zaměstnanci v dané společnosti požadována již při nástupu do zaměstnání. Fotografie je zobrazena na identifikační kartě zaměstnance, dále v informačním systému a každý zaměstnanec si ji libovolně může zvolit jako fotku u e-mailové pošty.

Společnost XX a. s. uvádí, že fotografie zaměstnanců využívá za účelem vnitřní komunikace a prezentace ve společnosti (jedná se např. o fotografie v telefonním seznamu, fotografie z interních společenských akcí vystavených v rámci společnosti). Za účelem jednoduššího čerpání benefitů u externích partnerů je umisťována fotografie na identifikační kartu. Díky tomu mohou partneři snáze ověřit identitu zaměstnance bez dalších dokladů.

Zaměstnanci společnosti mají povinnost zveřejnit fotografii v telefonním seznamu, což stálo v e-mailu, který byl rozesílán všem zaměstnancům. Bylo zde také uvedeno, jak by fotografie měla vypadat a jakým způsobem ji mají zaměstnanci do systému nahrát. Spoustě zaměstnancům se tento požadavek nelíbil a svou fotografii nezveřejnili do teď s odůvodněním, že je to narušování jejich soukromí.

Použití fotek zaměstnanců v rámci vnitřního systému společnosti za účelem identifikace oprávněných osob lze posoudit jako oprávněný zájem zaměstnavatele, o tom hovoří i článek 6 odst. 1 písm. f) GDPR. Pokud tedy zaměstnavatel požaduje fotografie zaměstnanců za účelem identifikace v rámci vnitřního systému společnosti, není třeba souhlas zaměstnance s využitím fotografie. Jiná situace nastává v okamžiku, kdy zaměstnavatel dostatečně neprokáže důvod (oprávněný zájem), měl by si zajistit souhlas zaměstnance (Podnikatel.cz, 2019).

4.5 Zpracování osobních údajů po ukončení pracovního poměru

Po ukončení pracovního poměru, ať už z podnětu zaměstnance či z podnětu společnosti, odpovídá personalista společnosti XX a. s. za dodržování všech ustanovení zákoníku práce vztahující se k důvodu a způsobu skončení pracovního poměru. Personalista je informován o ukončení přímým odpovědným vedoucím zaměstnance, vedoucí má také za úkol předat zaměstnanci příslušné dokumenty související s ukončením pracovního poměru, z nichž jedno vyhotovení musí být předáno zpět na útvar

Personalistika a mzdy. Personalista připraví Potvrzení o zaměstnání a na žádost zaměstnance vyhotoví Posudek o pracovní činnosti (na základě podkladů od vedoucího pracovníka) nejpozději do patnácti kalendářních dnů.

Personalista zašle odpovědnému vedoucímu písemnosti týkající se osobních údajů zaměstnance, pokud nemá uloženou povinnost v souladu s obecně závaznými předpisy tyto písemnosti archivovat. Dále zašle zaměstnanci formulář Vyrovnání závazků zaměstnance k zaměstnavateli s určením data, ke kterému je povinen tento formulář s potvrzením vyrovnání uvedených závazků předat zpět útvaru Personalistika a mzdy.

Do osobního spisu zaměstnance jsou založeny písemné dokumenty potvrzující ukončení pracovního poměru, vyplněný formulář Vyrovnání závazků zaměstnance a kopii zaměstnancem převzatého Potvrzení o zaměstnání, případně Pracovní posudek. Personalista provede po skončení pracovního poměru zaměstnance kontrolu obsahové úplnosti jeho osobního spisu a osobní spis vyřadí z evidence a uloží ho v souladu s vnitřním předpisem o archivaci a skartaci.

Společnost XX a. s. uvádí, že údaje bývalého zaměstnance jsou ukládány po nezbytně nutnou dobu. U údajů, které jsou součástí těch nejzásadnějších dokumentů (např. dokumenty o založení, zápisy z významných jednání, auditní zprávy, účetní uzávěrky), může být tato doba až neomezená, v některých zvláštních případech, např. údaje významné pro zaměstnancův důchod, musí společnost uchovat až 45 let. Podle zákona o bankách musí společnost uchovávat doklady o uskutečněných obchodech, na kterých může být zaměstnancovo jméno, pozice, kontakt i další detaily. Podle zákona o podnikání na kapitálovém trhu musí uchovávat údaje z evidence investičních nástrojů a všechny dokumenty týkající se údajů zapsaných v této evidenci 10 let od konce kalendářního roku, ve kterém byl údaj zapsán.

Společnost dále uvádí, že mezi údaje, u nichž jim zákon stanovuje kratší dobu uchování, patří například záznamy o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti (6 let), účetní podklady (5 let), stejnopisy evidenčních listů (3 roky) nebo daňové doklady (3 roky). Tyto a další údaje ale společnost obvykle archivuje po dobu 20 let z důvodu oprávněných zájmů, zejména pro případ, že by musela předkládat důkazy v soudním sporu.

4.6 Monitoring zaměstnanců

Společnost XX a. s. monitoruje své zaměstnance za účelem ochrany majetku a bezpečnosti a využívá k tomu několik různých postupů. Společnost respektuje soukromí svých zaměstnanců, ale zároveň trvá na tom, aby zaměstnanci používali poskytnuté prostředky komunikace vždy a na všech místech důstojným a odpovědným způsobem. Považuje za nezbytné stanovit určitá základní pravidla a principy, které mají zajistit důstojné a disciplinované využití těchto komunikačních prostředků. Proto je každému novému zaměstnanci na vstupním školení předána příručka s názvem Pravidla pro používání komunikačních prostředků ve společnosti XX a. s. Pravidla chování se vztahují na všechny komunikační prostředky poskytnuté zaměstnancům, jako jsou pevné a mobilní telefony, faxy, počítače, e-maily, internet atd.

Společnost také upozorňuje, že je povoleno využívat komunikační prostředky pouze pro plnění pracovních úkolů, pro interní komunikaci a externí komunikaci se zákazníky, dodavateli či státními orgány. Při případném soukromém využití je nutné respektovat pravidla stanovená vnitřními předpisy. Je zakázáno využívat přidělené komunikační prostředky pro zábavu. Společnost vytváří přihlašovací údaje a přístupová oprávnění, aby zaměstnanci měli k dispozici veškeré nástroje nezbytné k práci a společnost mohla přístupy spravovat a kontrolovat.

4.6.1 Kamerové systémy

Využívání kamerových systému patří v současnosti k nejčastěji využívanému prostředku k monitorování pracoviště a zaměstnavatelé je často využívají ke kontrole svých zaměstnanců, ani společnost XX a. s. není výjimkou. Kamerové systémy budov společnosti XX a. s. jsou instalovány v souladu s vnitřním předpisem Systém bezpečnostní technické ochrany. K používání kamerových systémů má také společnost k dispozici uživatelskou příručku nazvanou Ochrana osobních údajů při používání bezpečnostních kamerových systémů, která je v souladu s GDPR a stanovuje technicko-organizační opatření k zajištění ochrany osobních údajů klientů, návštěvníků, smluvních dodavatelů a zaměstnanců společnosti zaznamenaných kamerovými systémy instalovanými v objektech společnosti. Společnost dále uvádí, že předmětem ochrany jsou záznamy záběrů osob kamerovými systémy, a to bez ohledu na skutečnost, zda zaznamenané osoby jsou ze záběrů identifikovatelné či nikoli.

Kamerové systémy jsou instalovány za účelem ochrany osob a majetku společnosti proti protiprávnímu jednání. V zaměstnaneckých prostorách jsou také využívány k monitoringu dodržování bezpečnostních režimů při práci s hotovostí a ceninami, pro vstup a pobyt v zónách mimořádné a zvláštní důležitosti, pro vstup externích a dodavatelských pracovníků do prostor společnosti. Zaměstnanci jsou o kamerách instalovaných v zaměstnaneckých prostorách a o způsobu nakládání s pořízeným záznamem informováni prostřednictvím vnitřního předpisu.

Oznámení o zpracovávání osobních údajů kamerovými systémy podávají Úřadu pro ochranu osobních údajů pracovníci útvaru Bezpečnost na základě písemného pověření k této činnosti, vydaného statutárním orgánem společnosti.

Kamery jsou umístěny zejména u vstupu pro veřejnost, zaměstnance a v recepcích, v samoobslužné zóně, v bankovní hale a na pokladních pracovištích, v dotační místnosti, dotačním boxu a počítárně, v předtrezoří, v místnosti pro trezory a v komorovém trezoru, v pracovištích, kde se pracuje s hotovostí a jinými ceninami, na trasách přesunu hotovosti z centrální úschovy na pokladní pracoviště, ve výpočetních střediscích, datových archivech a u vstupu do místnosti instalace serveru IT, u vjezdů do objektů a na parkovištích. Kamery nejsou instalovány v kancelářských prostorách, šatnách a samozřejmě toaletách.

Kamery jsou instalovány veřejně (pouze u vstupů pro veřejnost jsou instalovány skrytě, a to s cílem zachycení pachatele loupežného přepadení při vstupu do bankovní haly). U některých objektů společnosti kamerové systémy obsluhují externí dodavatelé služby fyzické ostrahy, je s nimi uzavřena dohoda o ochraně informací. Společnost uvádí, že u veřejně instalovaných kamer jsou umístěny piktogramy

upozorňující na skutečnost, že daný prostor je sledován kamerami s pořizováním záznamu. Po prozkoumání jedné z budov společnosti, bylo zjištěno, že ne u všech kamer se piktogramy nachází. Tam kde byly, byla informace uvedena pouze v českém jazyce, chyběl zde údaj o správci zpracování a kontakt pro získání informací souvisejících se záznamem.

Vnitřní předpis zakazuje využívat záznamy kamerového systému ze strany vedoucích zaměstnanců k běžné kontrole činnosti podřízených zaměstnanců. Také je zakázáno využívat kamery vedoucími zaměstnanci či oprávněným zaměstnancem k objasňování pokladních schodků nebo jiných pochybení zaměstnanců pracujících s hotovostí či jinými ceninami a cennostmi. Pro tyto případy lze záznamy z kamerového systému využít výhradně cestou oprávněných útvarů společnosti nebo po podání trestního oznámení.

Záznam ze záznamových zařízení je uchováván výhradně lokálně, v místě instalace těchto zařízení. Ukládán je ve vlastním záznamovém zařízení. Není vedeno centrální úložiště záznamů z kamerových systémů. Záznamy jsou uchovávány po dobu 40 dnů od jejich pořízení, s výjimkou Výpočetních středisek – v těchto případech jsou záznamy z kamer uchovávány po dobu 90 dnů od jejich pořízení.

4.6.2 Přístup na internet a e-mailová pošta

Použití internetu a e-mailu nabízí značné výhody, pokud jde o efektivitu a přístup k informacím. Tyto komunikační prostředky mění pracovní zvyklosti a způsob, kterým společnost komunikuje a provádí obchody. Zaměstnanci společnosti XX a. s. jsou informováni, že by služební e-mail i internet měli využívat pouze k pracovním účelům. Společnost apeluje na své zaměstnance, že s rostoucím přístupem k internetu a stále intenzivnějším používám e-mailu je potřeba dodržovat pravidla s cílem:

- vyhnout se nežádoucímu chování (nezákonnému či nevhodnému použití),
- zaručit bezpečnost sítí a počítačových systémů,
- ochránit informace společnosti proti neoprávněnému rozšiřování,
- propagovat optimální a efektivní využití e-mailu.

Zaměstnanci mají k dispozici služební e-mail, který mohou využívat pouze k pracovním účelům. Předávání jakýchkoliv zpráv z počítače zaměstnance na jeho soukromou e-mailovou adresu je zakázáno. Je zakázáno čtení nebo zasílání zpráv prostřednictvím soukromých adres v rámci společnosti. Dále mají zaměstnanci povinnost odstranit všechny došlé e-mailové zprávy, které nejsou pracovního charakteru. Zaměstnanci jsou informování, že může být kontrolován odesílatel, příjemce a předmět zpráv, obsah zpráv společnost nekontroluje, výjimkou je e-mailová komunikace s klienty např. u zaměstnanců v Klientském centru.

Přístup k internetu ve společnosti XX a. s. je umožněn pouze, pokud je to nezbytné pro plnění pracovních úkolů. Zaměstnanec může navštěvovat pouze internetové stránky, které potřebuje k výkonu své práce. Je přísně zakázáno navštěvovat internetové servery obsahující pornografický, rasistický nebo jiný materiál. Dále je zakázáno umisťovat na webové stránky odkazy na WWW servery společnosti a její e-mailové adresy nebo schránky elektronické pošty. Některé internetové

stránky jsou přímo zablokovány a zaměstnancům na ně není umožněn přístup, zaměstnanci by také neměli z internetu do počítačů nic stahovat. Společnost informuje zaměstnance, že zpracovává osobní údaje vztahující se k chování na internetu, používá je pro účely hodnocení kybernetického rizika. Zaměstnancům je také sděleno, že mohou být kontrolovány IP adresy navštívených webových stránek.

4.6.3 Služební telefony

Většina zaměstnanců ve společnosti XX a. s. má na svém pracovním stole pevnou linku, kterou by měli využívat jen pro pracovní účely. Využít ji pro soukromé účely není zakázané, ale zaměstnanec by měl při soukromém využití zadat před vytáčené číslo dané předčíslí a úhrada za hovor je potom stržena z měsíční mzdy, což je ujednáno mezi zaměstnavatelem a zaměstnancem v dohodě o srážkách. Avšak zaměstnanci pevné linky dle vyjádření společnosti v dnešní době mobilů pro soukromé účely téměř nevyužívají.

Zaměstnanec si také může zažádat o přidělení mobilního zařízení pro služební i soukromé účely, mobilní zařízení přiděluje odpovědný vedoucí zaměstnanec. Mobilní zařízení se přidělují k pracovní pozici a nárok na toto zařízení zaniká okamžikem opuštění pracovní pozice bez náhrady. Zaměstnanec si zvolí typ tarifu, který požaduje, a dle tohoto výběru přispívá danou částkou, která mu je měsíčně strhávána ze mzdy, výběrem tarifu souhlasí se srážkou ze mzdy. Tímto nastavením nemá společnost potřebu kontrolovat využívání mobilních telefonů. Nedochází ani k monitorování hovorů s výjimkou u pracovních pozic, kde dochází ke komunikaci s klienty (především se jedná o Klientské centrum) a to za účelem zvyšování kvality služeb poskytovaných společností.

4.6.4 Služební automobily

Poskytování vozidla ve společnosti XX a. s. v rámci pracovní odměny (benefitu) je součástí nástrojů odměňování a je navázáno na konkrétní pracovní pozici manažera. Žádný manažer nemá na přidělení benefitního automobilu automatický nárok (přidělení musí být navrženo a schváleno v souladu s touto politikou). Řízení je možné i osobami v přímém příbuzenském vztahu – manžel/ka, syn, dcera, otec, matka, bratr, sestra, registrovaný partner. Vzhledem k tomu, že se jedná o benefit, není využívání automobilu nijak monitorováno.

Ostatním zaměstnancům jsou k dispozici automobily, pokud jedou na pracovní cestu či za klientem, v tomto případě může zaměstnanec využít automobil pouze pro služební účely. Tyto automobily jsou vybaveny GPS lokátorem a je tedy možné zpětně zmapovat skutečnou trasu. Zaměstnanci jsou o tomto systému v případě zapůjčení vozidla informováni a také jim je sděleno, že automobil nemohou využít k soukromým účelům.

4.6.5 Docházka

Dle § 96 ZP je zaměstnavatel povinen vést u jednotlivých zaměstnanců evidenci s vyznačením začátku a konce odpracované doby, což je podmíněno evidováním docházky. Způsob úpravy této problematiky není uložen, a tak je na zaměstnavateli, jaký způsob evidence docházky zvolí.

Společnost XX a. s. nemá striktní kontrolu pracovní docházky, neexistují zde žádné terminály, ke kterým by zaměstnanci přikládali své osobní karty. Každý zaměstnanec si tak sám zapisuje do elektronické docházkové knihy, kdy do práce přišel, v jaké době a jak dlouho měl pauzu a kdy z práce odešel. Eviduje se zde také dovolená, lékař a tzv. home office. Do docházky má přístup zaměstnanec, kterého se daná docházka týká, jeho přímý nadřízený a pracovníci Personalistiky a mzdy a útvaru HR. Ke konci měsíce odešle docházku za daný měsíc svému nadřízenému a ten by měl docházku zkontrolovat a odsouhlasit. Je tedy ponecháno na odpovědných vedoucích, zda a jak pečlivě příchody a odchody svých podřízených kontrolují.

4.7 Shrnutí

Společnost XX a. s. se při zpracování osobních údajů zaměstnanců a jejich monitoringu nedopouští žádného velkého pochybení. Jde vidět, že se snaží, aby nedocházelo k porušování legislativy, některá ustanovení jsou doplněna vnitřními předpisy a také má společnost vytvořenou celou řadu pomůcek a postupů, jak v této problematice postupovat. Dobře si uvědomuje, že soukromí zaměstnanců je potřeba chránit.

Osobní údaje jsou shromažďovány již od uchazečů výběrových řízení, což si společnost plně uvědomuje, a proto požaduje po uchazečích pouze takové údaje, které jsou nezbytné k naplnění účelu výběru uchazeče na volná pracovní místa. Zaměstnavatel po uchazečích nepožaduje žádné citlivé údaje a snaží se vyhýbat diskriminačním otázkám. Uchazeče o zpracování osobních údajů seznamuje pomocí textu prohlášení zpracování, které je k dispozici při registraci do databáze společnosti přes webové stránky. Jediným problémem je, že společnost nemá ošetřenou situaci, kdy zájemce o práci přinese životopis fyzicky.

Během trvání pracovního poměru zaměstnanců přibývají společnosti další údaje ke zpracování. Společnost chrání osobní data zaměstnanců před zneužitím pomocí uzamykatelných skříní, co se týká dat v listinné podobě, v elektronické podobě jsou data chráněna především díky přístupovým oprávněním. O každém zaměstnanci je veden osobní spis, kde jsou ukládány nezbytně nutné údaje a o tyto spisy se stará útvar Personalistiky a mzdy. Nedostatkem je, že zaměstnanci tohoto útvaru nenavštěvují školení týkající se této problematiky a také nedostatečné informování zaměstnanců o nakládání s jejich údaji a o jejich právech. Kvůli nedostatečnému informováni potom mohou vznikat neshody, jako to bylo např. u zveřejnění fotografie.

Po ukončení pracovního poměru se zaměstnancem společnost archivuje některé dokumenty, a to buď z důvodu oprávněných zájmů, nebo proto, že jim to stanovuje zákon.

Ve společnosti XX a. s. dochází také k monitorování zaměstnanců. Společnost hojně využívá kamerových systémů. Zaměstnavatel informuje své zaměstnance, že je jejich prostor monitorován pomocí vnitřního předpisu, povinnost informovat mu ukládá právní předpis. Dále legislativa říká, že by všechny kamery měly být řádně označeny, ale bylo zjištěno, že některé z kamer označeny vůbec nejsou, bylo by tedy vhodné v tomto případě sjednat nápravu.

Společnost uchovává kamerové záznamy po dobu 40 dnů (u Výpočetních středisek po dobu 90 dnů) od jejich pořízení. ÚOOÚ (2018) uvádí: *„Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Uchovávaná data by měla být uchovávána v rámci časové smyčky např. 24 hodin, pokud jde o trvale střežený objekt, nebo případně i dobu delší, v zásadě však nepřesahující několik dnů, nejde-li o pořizování záznamů policejním orgánem podle zvláštního zákona, a po uplynutí této doby vymazána.“*. Dle uvedeného by se společnost měla zamyslet, zda neuchovává záznamy příliš dlouho.

Co se týká ostatního monitoringu ve společnosti, dá se konstatovat, že společnost kontroluje své zaměstnance přiměřeně a postupuje dle platné legislativy.

5 Návrhy a doporučení

V předchozí kapitole byl popsán postup zpracování osobních údajů a monitoring zaměstnanců ve společnosti XX a. s. Tato část měla ukázat, jakým způsobem společnost nakládá s osobními daty v běžné každodenní situaci. Bylo zjištěno, že společnost se o problematiku ochrany osobních údajů svých zaměstnanců zajímá, věnuje této oblasti dost pozornosti a snaží se postupovat dle platných právních předpisů. I přesto uvedu v této kapitole nějaké návrhy a doporučení, které by mohla společnost využít a zlepšit tak současné postupy týkající se osobních údajů zaměstnanců.

5.1 Souhlas se zpracováním osobních údajů

Jak bylo řečeno, může se uchazeč o zaměstnání přihlásit do výběrového řízení pomocí registrace do databáze společnosti přes webové stránky společnosti, kde odsouhlasí, že se seznámil s prohlášením o ochraně osobních dat. Společnost nemá ale nijak ošetřenu situaci, když uchazeč přinese životopis fyzicky a odevzdá ho např. na pobočce.

Bylo by tedy přínosné, když by měla společnost přichystaný vytisknutý text prohlášení a souhlasu zpracování osobních údajů, aby se uchazeč mohl seznámit s tím, jak bude nakládáno s jeho údaji a dát k tomu souhlas. I když legislativa přímý souhlas přímo nevyžaduje, společnost by tím předešla případným neshodám a komplikacím.

Řešení tohoto návrhu není nijak složité ani finančně náročné. Text prohlášení (seznámení s osobními údaji) má společnost už připravený elektronicky, stačí ho jen vytisknout a na útvaru Personalistika a mzdy by k tomu připravili jednoduchý text, kde by uchazeč potvrdil svůj souhlas podpisem a případně by zvolil možnost, zda chce, aby jeho údaje byly použitý pouze pro konkrétní výběrové řízení nebo i pro další. Text by mohl vypadat nějak takto: *„Já …… (jméno uchazeče) potvrzuji, že jsem se seznámil/a s textem zpracování osobních údajů a souhlasím s tím, aby mé osobní údaje byly zpracovávány společností XX a. s. za účelem konkrétního výběrového řízení / konkrétního výběrového řízení a zároveň souhlasím, abych byl osloven i s dalšími pracovními nabídkami v rámci společnosti XX a. s. (nehodící se škrtněte). Já níže podepsaný uděluji svůj souhlas svobodně a dobrovolně.“* Pod tímto textem by bylo místo a datum podpisu a podpis osoby.

Tyto texty by byly připraveny na každé pobočce a příslušní zaměstnanci by byli seznámeni s tím, že každý zájemce o zaměstnání se musí s textem prohlášení seznámit a podepsat souhlas. Následně by odpovědný zaměstnanec na pobočce přisvorkoval souhlas k dokumentům od uchazeče (životopis, motivační dopis) a předal by to vše specialistovi útvaru Náboru.

Náklady na toto řešení jsou považovány za minimální. Na každém oddělení je k dispozici tiskárna, proto není pro společnost tisk textů drahý ani komplikovaný. Zaměstnanci pobočky by měli být seznámeni, jak postupovat, pokud uchazeč přinese svůj životopis na pobočku. Krátké školení by mohli provést zaměstnanci útvaru Náboru.

Tab. 1 Kalkulace nákladů na formulář souhlasu se zpracováním osobních údajů

Náklady na tisk textů	0,40 Kč / A5
Hodinová mzda zaměstnance útvaru Náboru	250 Kč

Zdroj: interní

Toto opatření je o dost jednodušší a méně nákladnější, než když by se společnost dostala do sporu s uchazečem, který by ji nařknul za nedodržování právních předpisů. Společnost by poté musela řešit situaci s dozorovým orgánem, případně si najmout obhájce a v nejhorším případě platit sankce.

5.2 Školení zaměstnanců

Z důvodu rychlého rozvoje technologie a častých útoků do soukromí jednotlivce, je v současnosti ochrana osobních údajů velmi řešeným tématem a v právních předpisech dochází ke změnám. Proto by měla společnost XX a. s. dbát na to, aby zaměstnanci útvaru Personalistika a mzdy, HR útvaru a útvaru Náboru byli dostatečně obeznámeni se všemi změnami právních předpisů a postupovali správným způsobem.

Bohužel bylo zjištěno, že společnost sice vydává různé vnitřní předpisy, pomůcky a návody, kde si zaměstnanci mohou přečíst o tom, jak správně postupovat v souladu s legislativou, ale nikdo je už je s touto problematikou detailně neseznámí.

Dle mého názoru by měli zaměstnanci těchto útvarů navštěvovat školení týkající se této problematiky každý rok, ať už je něco nového nebo není, buď se dozví o nových věcech, anebo si jen „osvěží“ to, co od minule zapomněli. Zaměstnanci těchto útvarů se s osobními údaji potýkají velmi často, a proto je důležité, aby veškeré jejich kroky byly správné a společnosti tak nehrozili sankce za jejich pochybení, které by mohly být několikanásobně vyšší než školení.

Jednalo by se o celodenní externí školení, které by zaměstnanci výše uvedených útvarů navštívili postupně během roku. Částka je tedy nejdříve uvedena za jednoho zaměstnance, ale protože dohromady v těchto útvarech pracuje zhruba 65 zaměstnanců, je částka vyčíslena za všechny zaměstnance dohromady. Vypočítaná částka se může zdát na první pohled příliš vysoká, ale sankce za porušení legislativy může vyšplhat až do výše desítek milionu EUR a v porovnání s tím, je cena za školení minimální.

Tab. 2 Kalkulace nákladů za školení zaměstnanců

	Jednotkové náklady	**Celkem / za rok**
Školení v oblasti zpracování osobních údajů zaměstnanců	1990 Kč	**129 350 Kč**

Zdroj: TSM vzdělávací agentura, 2019

Po rozhovoru s některými ze zaměstnanců mimo výše uvedené útvary bylo zjištěno, že nejsou příliš dobře informováni o svých právech subjektů údajů. Navrhovala bych

tedy zlepšit toto informování, obzvlášť vždy po tom, co dojde k nějaké změně v právních předpisech. Minimálně by mohla společnost rozesílat informace o změnách v této oblasti e-mailem, především když má k dispozici vnitřní předpisy týkající se této problematiky. Nově nastupující zaměstnanci musí projít celodenním vstupním školením, kde jim jsou sdělovány různé informace, nějaký prostor by mohl být věnován právě problematice ochrany osobních údajů. Školení by bylo zhruba hodinové a mohl by je vést zaměstnanec útvaru Personalistika a mzdy. Jediným nákladem by potom byla pouze hodinová mzda školitele – 250 Kč (interní zdroj).

5.3 Správné označení kamerového systému

Společnost XX a. s. využívá hojně kamerový systém ve všech svých budovách. Jak již bylo řečeno, povinností správce osobních údajů provozující kamerový systém je řádně označit tyto kamery piktogramem, kde stojí informace o monitorování objektu, kdo je správce údajů a případně kontakt na něj.

Bylo zjištěno, že společnost nemá všechny kamery řádně označené, u některých chybí upozornění o monitorování úplně, u jiných je sice piktogram, ale chybí údaje o správci. Navíc informace jsou pouze v českém jazyce a jelikož společnost navštěvuje i spousta cizinců, bylo by vhodné uvádět dané informace minimálně i v jazyce anglickém. Aby bylo označení všude stejné, bylo by nejlepší vytvořit nové označení pro všechny budovy.

Do nákladů na pořízení se řadí tabulka s piktogramem a s informacemi o správci v českém jazyce a druhá tabulka v jazyce anglickém, dále instalace tabulek, kterou by provedl zaměstnanec společnosti XX a. s. mající na starost správu budov. Překlad informací do anglického jazyka není potřeba řešit, jelikož se dají koupit rovnou už předpřipravené tabulky v cizím jazyce. Materiál tabulek je dle výrobce PVC odolný vůči vlivům počasí, proto se dají tabulky použít vevnitř i vně budovy (safetyshop.cz, 2019). Předpokládaná kalkulace je provedena na jednu budovu, průměrně je v jedné budově využito patnáct kamer.

Tab. 3 Kalkulace nákladů na označení kamerového systému

	Náklady na jeden kus	**Náklady na budovu**
Tabulka v českém jazyce	59,29 Kč	889,35 Kč
Tabulka v anglickém jazyce	69,29 Kč	1039,35 Kč
Poštovné	90 Kč	90 Kč
Hodinová mzda správce za instalaci tabulek v jedné budově (3 h)		350 Kč
Celkem		**2368,7 Kč**

Zdroj: safetyshop.cz, 2019

Obr. 2 Správná podoba piktogramu kamerového systému
Zdroj: safetyshop.cz, 2019

Jak již bylo uvedeno, společnost XX a. s. uchovává kamerové záznamy po dobu 40 dnů (u Výpočetních středisek po dobu 90 dnů) od jejich pořízení. Ale doba uchovávání by neměla být delší, než je třeba pro naplnění účelu a v zásadě by neměla přesáhnout několik dní. Doporučovala bych tedy společnosti zkrátit lhůty uchovávání minimálně na polovinu, taková doba by měla být dostačující pro účel ochrany osob a majetku společnosti proti protiprávními jednání, který uvádí společnost ve svém vnitřním předpise o kamerových systémech.

Dále bych chtěla zmínit, že společnost ve vnitřním předpise uvádí, že zaměstnanci útvaru Bezpečnost podávají Úřadu pro ochranu osobních údajů oznámení o zpracování osobních údajů kamerovými systémy. Dle ÚOOÚ (2018) byla registrace kamerových systémů u ÚOOÚ ukončena. Úřad uvádí, že Obecné nařízení registrační povinnost již neukládá na rozdíl od již neplatného zákona o ochraně osobních údajů. Je tedy zbytečné, aby se zaměstnanci společnosti zabývali touto prací, když vynaložené úsilí mohou využít někde jinde.

5.4 Zpracování fotografií

Bylo zjištěno, že společnost XX a. s. ukládala svým zaměstnancům za povinnost zveřejnit si fotografii v telefonním seznamu a spousta zaměstnanců s tím nesouhlasila.

I když se zpracování fotografie dá vyhodnotit jako oprávněný zájem zaměstnavatele dle článku 6 odst. 1 písm. f) GDPR a není tedy nutný výslovný souhlas zaměstnance, nemůže zaměstnavatel zaměstnance nutit. Podle odst. 11 čl. 4 GDPR musí být souhlas subjektu údajů svobodný. Zaměstnanec má také právo vznést námitku proti zpracování jeho osobních údajů dle odst. 1 čl. 21 GDPR a také může svůj souhlas se zpracováním údajů odvolat a domáhat se práva o výmaz (odst. 1 čl. 17 GDPR).

V první řadě by bylo dobré vysvětlit zaměstnancům svůj záměr a odkázat se na příslušnou legislativu. Zaměstnanci by neměli být do něčeho nuceni bez toho, aby byli dostatečně informováni, o tom hovoří i odst. 1 čl. 12 GDPR.

Společnost by měla zvážit, zda je nutné po zaměstnancích zveřejnění fotografie požadovat, a to z důvodu respektování osobnostního práva a zachování dobrých vztahů se zaměstnanci. Pokud by společnost na fotografii trvala, bylo by vhodné nejprve si vyžádat od zaměstnanců jejich souhlas, aby se společnost vyhnula zbytečným komplikacím a konfliktům. Souhlas by mohl být formulován zhruba takto: *„Já, níže podepsaný/á ……., souhlasím s tím, aby společnost XX a.s. využívala moji fotografii za účelem vnitřní komunikace, prezentace ve společnosti a identifikace osob v rámci společnosti. Souhlas je platný pouze v případě dosažení účelu zpracování a v souladu s platnou legislativou. Byl/a jsem poučen/a o svých právech jako subjekt údajů. Souhlas uděluji svobodně a dobrovolně.“* Pod tímto textem by bylo uvedeno místo a datum podpisu a podpis osoby.

U nově nastupujících zaměstnanců by jim byl formulář souhlasu předán k podpisu hned při požadavku předložit základní doklady nutné pro vznik pracovního poměru. Získání souhlasu, od již stávajících zaměstnanců, by měl na starost útvar Personalistika a mzdy a po podepsání souhlasu by byl dokument přidán do osobního spisu zaměstnance. Náklady na toto získání souhlasu jsou minimální, jedná se o vytisknutí formuláře (0,40 Kč / A5, interní zdroj), a to pouze u stávajících zaměstnanců, u nových zaměstnanců by byl formulář zasílán s ostatními dokumenty elektronicky. Dále je to mzda zaměstnance útvaru Personalistika a mzdy, která je vyčíslena ve výši 250 Kč za hodinu (interní zdroj).

6 Diskuse

Ochrana osobních údajů se především v posledních letech stala vysoce diskutovaným tématem v pracovněprávních vztazích, příčinou bylo nahrazení zákona č. 101/2000 Sb., ZoOOÚ Obecným nařízením. Zpracování osobních údajů zaměstnance je velmi obsáhlé téma. Právní předpisy udávají zásady zpracování osobních údajů, práva a povinnosti správce i subjektu údajů, řeší sankce a pokuty za porušení některé ze stanovených povinností. Součástí legislativy jsou také možnosti monitoringu pracoviště. Podnik by měl mít znalost zákonů, jako je GDPR, občanský zákoník, zákoník práce atd. a mel by vždy postupovat v souladu s těmito předpisy. Společnost by vždy měla shromažďovat jen nezbytně nutné osobní údaje, stanovit účel sběru dat a neuchovávat je déle, než je třeba.

Při výběrovém řízení nastává první zpracování osobních údajů potenciálních zaměstnanců. Přijímání nových zaměstnanců lze rozdělit do fází: přihlášení uchazeče do výběrového řízení, samotné výběrové řízení a jeho ukončení. Každý uchazeč by měl být informován o zpracování jeho osobních údajů a měl by potvrdit, že byl s touto problematikou seznámen. Společnost XX a. s. má seznámí se zpracováním ošetřeno v případě, kdy se uchazeč přihlašuje do výběrového řízení přes jejich webové stránky, nedořešenou má společnost situaci, kdy uchazeč přinese svůj životopis osobně. Řešením by bylo mít připravené a vytisknuté seznámení se zpracováním osobních údajů na pobočkách společnosti, kde by příslušní zaměstnanci předali tento text uchazeči k nastudování a uchazeč by svůj souhlas stvrdil podpisem. Tím by byla splněna základní povinnost zaměstnavatele informovat subjekty údajů.

Nebylo zjištěno žádné pochybení při vykonávání výběrového řízení, společnost XX a. s. apeluje na své zaměstnance útvaru Nábor, aby se vyhnuli diskriminačním otázkám, které zákon zakazuje. Po ukončení výběrového řízení zákon povoluje ponechat si poskytnuté životopisy pro potřeby dalšího využití pouze se souhlasem dotčených osob, kterým musí být znám účel a doba nového využití. To má společnost ošetřeno již při přihlašování uchazeče do výběrového řízení přes webové stránky, kde každý zájemce zvolí, zda chce, aby jeho údaje byly využity pouze pro konkrétní výběrové řízení anebo i pro další pracovní nabídky.

V případě výběru vhodného kandidáta má zaměstnavatel povinnost seznámit jej s právy a povinnostmi vyplývajícími z pracovní smlouvy, s pracovními podmínkami a podmínkami odměňování. Pokud uchazeč pracovní nabídku přijme, musí předložit základní doklady nutné pro vznik pracovního poměru, tyto doklady jsou následně uloženy do osobní složky zaměstnance. Dále by zaměstnanci měli být informování o svých právech subjektů údajů, a to jak noví zaměstnanci při nástupu do společnosti, tak i současní zaměstnanci v případě nějaké změny v legislativě. Společnost sice disponuje vnitropodnikovými směrnicemi týkající se této problematiky, ale většina zaměstnanců o tom nemá ani povědomí, a proto by měla společnost tento nedostatek napravit, například informováním současných zaměstnanců pomocí e-mailu či jednorázovým školením při nástupu do zaměstnání.

Zákoník práce uvádí, že zaměstnavatel smí po zaměstnanci požadovat pouze takové údaje, které jsou nezbytné pro výkon práce v pracovněprávním vtahu. A zákon také nepožaduje souhlas zaměstnance se zpracováním osobních údajů, jelikož zaměstnavatel musí zpracovávat osobní údaje ke splnění povinností dle pracovní smlouvy, na které je pracovní vztah založen. Společnost není v této záležitosti v rozporu a uvádí, že osobní údaje získává na základě dobrovolného rozhodnutí zaměstnance a tyto údaje jsou požadovány z důvodu oprávněného zájmu. Jediný problém ve společnosti XX a. s. nastal při zpracování fotografií zaměstnanců, kdy společnost svým zaměstnancům ukládala povinnost zveřejnit své fotografie v telefonním seznamu, ale mnoho zaměstnanců s tím nesouhlasilo. Společnost by měla tento svůj postoj zvážit v rámci respektování osobnostního práva a k udržení dobrých pracovních vztahů.

Společnost XX a. s. využívá k ulehčení zpracování osobních údajů svých zaměstnanců informační systém SAP, kde jsou uchovávány dokumenty v elektronické podobě. Společnost velmi dbá na ochranu osobních údajů zaměstnanců, proto do informačního systému mají přístup pouze zaměstnanci útvaru Personalistika a mzdy a HR, dále zaměstnance, kterého se osobní údaje týkají. Systém není webový, díky čemuž je chráněn proti útokům na osobní údaje zvenčí. Do daného systému, a i do dalších interních databází, jsou zaměstnancům přidělována přístupová oprávnění a přihlašovací údaje a společnost na zaměstnance apeluje, aby uzamykali při odchodu svůj počítač, aby byl zamezen přístup nepovolaným osobám.

Data v listinné podobě ukládá společnost v uzamykatelných skříních v kancelářích útvaru Personalistika a mzdy a mají k nim přístup pouze pracovníci tohoto útvaru. Pro zabezpečení je také využíván systém identifikačních karet, ke každé kartě jsou nastavována vstupní práva individuálně v závislosti na pracovní pozici. Jsou vyhrazeny konkrétní prostory, do nichž mají právo vstoupit pouze oprávněné osoby. Ochrana je také podpořena povinností mlčenlivosti, která se vztahuje na zaměstnance zpracovávající údaje. Shrneme-li zabezpečovací prvky, které společnost využívá, dá se konstatovat, že všechny opatření jsou využívána pozorně a pečlivě. Jako nedostatek bylo pouze zjištěno to, že zaměstnanci společnosti zpracovávající osobní údaje nejsou pravidelně seznamováni se změnami v této problematice či nepodstupují pravidelná školení. Toto zjištění by měla společnost napravit a zamyslet se nad nápravou, aby společnosti nehrozily zbytečné sankce za případné pochybení zaměstnanců.

Na pracovišti může docházet ke střetu zájmů zaměstnavatele a zaměstnance. Na jedné straně je zaměstnanec s povinností řádně plnit své pracovní povinnosti a právem na soukromí a na druhé straně zaměstnavatel s právem kontrolovat plnění pracovních povinností a chránit svůj majetek a bezpečnost. Zákon zaměstnavateli dovoluje přiměřeně kontrolovat své zaměstnance, ale nesmí bez závažného důvodu narušovat soukromí zaměstnance. Společnost XX a. s. využívá všechny monitorovací systémy s ohledem na práva a soukromí zaměstnanců, jediným nedostatkem je nesprávné označení kamerového systému, což by bylo vhodné napravit, aby bylo vše v souladu s legislativou. Dále by bylo vhodné se zamyslet nad zkrácením lhůty uchovávání kamerových záznamů, jelikož zákon říká, že doba uchování by neměla být delší, než je třeba pro naplnění účelu a v zásadě by neměla přesáhnout několik dní.

Na základě analýzy jednotlivých postupů zpracování osobních údajů ve společnosti XX a. s. byly zjištěny mírné nedostatky, které by měly být napraveny. Především se jedná o vylepšení získání souhlasu se zpracováním osobních údajů, lepší informovanost zaměstnanců jako subjektů údajů, školení zaměstnanců zpracovávajících osobní údaje a řádně označit kamerový systém. Nákladovost těchto opatření nedosahuje velkých částek, jedná se o režijní náklady související s tiskem formulářů a odměnou pro zaměstnance zpracovávající tento úkol. Dále se jedná o náklady za školení v oblasti zpracování osobních údajů, tyto náklady jsou o poznání vyšší, ale v porovnání se sankcemi, které by mohly společnosti hrozit za chyby zaměstnanců, z důvodu nedostatečné informovanosti, jsou minimální. Náklady za správné označení kamerového systému jsou jednorázové a nejsou natolik výrazné, aby narušily finanční plán podniku. Společnost nápravnými opatřeními předejde potenciálním stížnostem za zpracování osobních údajů a ochrání si tak dobré jméno společnosti.

Doporučení, nad kterým by se měla společnost zamyslet, je požadování zveřejnění fotografií po zaměstnancích, i když s tím nesouhlasí. Jednání společnosti se sice dá v rámci legislativy vysvětlit jako oprávněný zájem, ale souhlas zaměstnance se zpracováním údajů musí být svobodný a společnost by neměla zaměstnance nutit. Jednáním společnosti by mohlo dojít ke zbytečným konfliktům a narušení dobrých vztahů mezi zaměstnavatelem a zaměstnanci.

Po zhodnocení všech získaných informací se dá konstatovat, že společnost XX a. s. má dobře nastavenou ochranu osobních údajů zaměstnanců, má vytvořenou celou řadu vnitřních předpisů, postupů a pomůcek. Jedná se o velice dobře nastavený systém podmínek pro zpracování údajů. Společnost si uvědomuje, že soukromí zaměstnanců je potřeba chránit a snaží se postupovat dle platné legislativy. Ve společnosti nedochází v této oblasti k žádnému velkému pochybení, byly zjištěny spíše drobné nedostatky, které by bylo vhodné napravit pro zachování dobrého chodu společnosti i v budoucnu.

7 Závěr

Diplomová práce se věnovala tématu ochrana osobních údajů a soukromí zaměstnance v obchodní společnosti. Hlavním cílem bylo na základě analýzy vyhodnotit úroveň ochrany soukromí a osobních údajů zaměstnanců ve vybrané společnosti, identifikovat případné nedostatky a navrhnout doporučení či zlepšení již používaných procesů. Dílčím cílem byla aplikace legislativy na procesy ve společnosti a také ekonomické vyčíslení případných doporučení.

Ochrana osobních údajů a ochrana soukromí je důležitým tématem, které je s člověkem spojeno po celý jeho život v mnoha situacích. Osobní údaje a soukromí se vyvíjí již dlouhou řadu let, ale především v současnosti ochrana údajů a soukromí nabývá na síle a je to čím dál častěji řešené téma, převážně díky velkému rozvoji technologií.

V literární rešerši jsou nejprve představeny hlavní prameny týkající se ochrany osobních údajů, je nastíněn vývoj těchto pramenů a také je představena nejnovější právní úprava, a to Obecné nařízení o ochraně osobních údajů. Poté jsou vymezeny důležité pojmy týkající se dané problematiky, které celou práci provázejí. Podrobně jsou popsány zásady zpracování osobních údajů, sankce a pokuty za porušení povinností. Důležitou součástí je dozorový úřad, který dohlíží na uplatňování právních předpisů, v České republice funkci dozorového úřadu plní Úřad pro ochranu osobních údajů. V druhé části literární rešerše je řešen způsob zpracování osobních údajů celé časové řady pracovního vztahu, tzn. před uzavřením pracovního poměru, v jeho průběhu a po jeho ukončení. Jsou popsána s tím související práva a povinnosti zaměstnavatele a zaměstnance. A následně je diskutována oprávněnost monitoringu pracoviště.

Vlastní práce se zabývá analýzou ochrany soukromí a osobních údajů zaměstnanců ve vybrané společnosti. Společnost je zkoumána v anonymizované podobě, vystupuje jako společnost XX a. s. Činnosti společnosti související se zpracováním osobních údajů jsou v této části porovnávány s právními předpisy, což následně tvoří zdroj pro návrhy a doporučení.

Zpracování osobních údajů a ochrana soukromí jsou ve společnosti sledovány již před uzavřením pracovněprávního vztahu, a to od přihlášení uchazeče do výběrového řízení, přes samotné výběrové řízení a následné nakládání s informacemi o neúspěšných uchazečích. Ve výběrovém řízení je zvolen vhodný uchazeč, od kterého jsou získávány další osobní údaje při uzavření pracovní smlouvy a potřebné k jejímu plnění. Konečnou fází je nakládání s osobními údaji po ukončení pracovního poměru, jejich archivace a následná likvidace. Důležitou součástí je také monitoring zaměstnanců a jejich pracovišť, který společnost provozuje. Jedná se především o kamerový systém, docházkový systém a využívání svěřených pracovních prostředků zaměstnanci.

Při analýze postupů ve společnosti XX a. s. bylo zjištěno, že společnost má ochranu soukromí a osobních údajů zaměstnanců dobře nastavenou. Jedná se o velkou společnost s dostatečnými prostředky na to, aby zpracování osobních údajů fungovalo dle legislativy a společnost byla schopna poměrně rychle reagovat

na změny v právních předpisech. Společnost se snaží respektovat osobnostní práva zaměstnanců a udržovat dobré pracovní vztahy. Velikost podniku také nutí vedení k tomu, aby veškeré kroky a postupy byly v souladu se zákonem, jelikož případné konflikty by mohly poškodit dobré jméno společnosti. I přesto bylo zjištěno několik drobných nedostatků, proto je v závěru věnována kapitola doporučení, jejichž realizací by společnost předešla sporům se zaměstnanci, stížnostem a případným sankcím od dozorového úřadu. Jedná se o chybějící souhlas se zpracováním osobních údajů v případě, kdy uchazeč přinese životopis osobně, lepší informovanost zaměstnanců o jejich právech jako subjektech údajů, školení zaměstnanců zpracovávající údaje, správné označení kamerového systému a zvážení zpracování fotografií zaměstnanců. Doporučení jsou i ekonomicky vyčíslena. Výsledné náklady na realizaci nápravných opatření jsou považovány za minimální oproti problémům a pokutám, které by společnosti mohly hrozit v případě porušení některé z povinností.

Obsah práce může být přínosem nejen pro společnost XX a. s., ale třeba i pro jiné podniky. Informace uvedené v obou částech práce mohou sloužit jako pomoc pro vnitropodnikové procesy jiných firem.

8 Literatura

BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012*. Olomouc: ANAG, 2012. Právo (ANAG). ISBN 978-80-7263-749-2.

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.

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

JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.

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.

KENYON, Andrew T. a Megan RICHARDSON. *New dimensions in privacy law: international and comparative perspectives*. New York: Cambridge University Press, 2006. ISBN 0-521-86074-1.

KLÍMA, Karel a Markéta ŠÁLENÁ. *Ústavní právo*. Dobrá Voda u Pelhřimova: Aleš Čeněk, 2002. Právnické učebnice (Aleš Čeněk). ISBN 80-86473-20-1.

MATES, Pavel. *Ochrana soukromí ve správním právu*. 2., aktualiz. a podstatně přeprac. vyd. Praha: Linde, 2006. ISBN 80-7201-589-3.

MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. *Ochrana osobních údajů*. Praha: Leges, 2012. Praktik (Leges). ISBN 978-80-87576-12-0.

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

NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.

NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018. Komentátor. ISBN 978-80-7502-288-2.

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.

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

ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3.

Internetové zdroje

BURIAN, David. *K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR)* [online]. 2016 [cit. 2019-10-07]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr.

Evropská komise. *Co jsou to úřady pro ochranu osobních údajů?* [online]. 2018 [cit. 2019-10-15]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_cs.

CHLEBUS, Tomáš. *Nový zákon o zpracování osobních údajů* [online]. 2019 [cit. 2019-10-07]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html.

KUBÍČKOVÁ, Alice a Veronika PATÁKOVÁ. *Ochrana osobních údajů zaměstnanců od A (přes GDPR) do Z.* [online]. 2017 [cit. 2019-10-28]. Dostupné z: https://www.praceamzda.cz/clanky/ochrana-osobnich-udaju-zamestnancu-od-pres-gdpr-do-z.

MARCÍN, Vojtěch. *Zpracování fotografií zaměstnanců vyžaduje opatrnost. Na co si dát pozor?* [online]. 2019 [cit. 2019-12-04]. Dostupné z: https://www.podnikatel.cz/clanky/zpracovani-fotografii-zamestnancu-vyzaduje-opatrnost-na-co-si-dat-pozor/

RADIČOVÁ, Zuzana a David BURIAN. *Nová regulace ochrany osobních údajů aneb na jaké změny se připravit* [online]. 2016 [cit. 2019-10-07]. Dostupné z: https://www.epravo.cz/top/clanky/nova-regulace-ochranyosobnich-udaju-aneb-na-jake-zmeny-se-pripravit-103479.html.

Safetyshop.cz. *Kamerový systém* [online]. 2019 [cit. 2019-12-04]. Dostupné z: https://www.safetyshop.cz/c320-kamerovy-system.

ŠKUBAL, Jaroslav a Tomáš LIŠKUTÍN. *Okamžité zrušení pracovního poměru se zaměstnancem za prohlížení internetu* [online]. 2012 [cit. 2019-10-28]. Dostupné z: https://www.epravo.cz/top/clanky/okamzite-zruseni-pracovniho-pomeru-se-zamestnancem-za-prohlizeni-internetu-85215.html.

TAHOTNÁ, Lucie. *Zaměstnavatel jako správce osobních údajů zaměstnanců* [online]. 2017 [cit. 2019-10-21]. Dostupné z: https://www.epravo.cz/top/clanky/zamestnavatel-jako-spravce-osobnich-udaju-zamestnancu-105934.html.

TSM vzdělávací agentura. *Nabídka kurzů* [online]. 2019 [cit. 2019-12-04]. Dostupné z: https://www.tsmvyskov.cz/nabidka-kurzu

Úřad pro ochranu osobních údajů. *K provozování kamerových systémů* [online]. 2018 [cit. 2019-12-04]. Dostupné z: https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099.

Úřad pro ochranu osobních údajů. *Zaměstnavatel jako správce osobních údajů* [online]. 2013 [cit. 2019-10-21]. Dostupné z: https://www.uoou.cz/zamestnavatel-jako-spravce-osobnich-udaju/d-6171.

Úřad pro ochranu osobních údajů. *Zaměstnavatelé* [online]. 2013 [cit. 2019-10-21]. Dostupné z: https://www.uoou.cz/zamestnavatele/ds-5057.

Úřad pro ochranu osobních údajů. *K provozování kamerových systémů* [online]. 2018 [cit. 2019-10-28]. Dostupné z: https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535.

Úřad pro ochranu osobních údajů. *Zásady a právní důvody zpracování* [online]. 2017 [cit. 2019-10-28]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271.

WARREN, Samuel a LOUIS Brandeis. *The Right to Privacy*. Harvard Law Review, 1890 [online]. [cit. 2019-10-7]: Dostupné z: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Why SAP? *SAP* [online]. 2019 [cit. 2019-12-04]. Dostupné z: https://www.sap.com/why-sap.html.

Právní předpisy

Listina základních práv a svobod. Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb. [online]. 1992 [cit. 2019-10-07]. Dostupné z: http://zakony.centrum.cz/listina-zakladnich-prav-a-svobod/hlava-1-clanek-2?full=1.

Zákon č. 262/2006 Sb., zákoník práce [online]. 2006 [cit. 2019-10-07]. Dostupné z: http://zakony.centrum.cz/zakonik-prace/cast-13-hlava-7-paragraf-313?full=1.

Zákon č. 110/2019 Sb., o zpracování osobních údajů [online]. 2019 [cit. 2019-10-07]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110.

Zákon č. 89/2012 Sb., občanský zákoník [online]. 2012 [cit. 2019-10-07]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89#cast1.

Zákon č. 435/2004 Sb., o zaměstnanosti [online]. 2004 [cit. 2019-10-28]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-435.

Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení [online]. 1991 [cit. 2019-10-28]. Dostupné z: https://www.zakonyprolidi.cz/cs/1991-582.