

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH
STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE**

BAKALÁŘSKÁ PRÁCE

**JURISTICKÉ ASPEKTY OCHRANY OSOBNÍCH
ÚDAJŮ VE VÝROBNÍ SPOLEČNOSTI**

Autor práce: Olga Jandová

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Bc. Josef Kříha

Katedra: Právních oborů a bezpečnostních studií

2018

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucímu bakalářské práce Mgr. Bc. Josefu Křihovi, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

JANDOVÁ, O. *Juristické aspekty ochrany osobních údajů ve výrobní společnosti: bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2018. 78 s. Vedoucí bakalářské práce: Mgr. et Bc. Josef Kříha.

Klíčová slova: osobní údaje, ochrana osobních údajů, subjekt údajů, správce a zpracovatel osobních údajů

Bakalářská práce (dále jen „práce“) má ambice formou teoreticko-praxeologického vhledu osvětlit aplikaci jednotlivých ustanovení aktuálně účinného zákona číslo 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů ve znění pozdějších předpisů. Práce pojednává o ochraně osobních údajů a povinnostech z toho plynoucích, a to z pohledu tzv. GDPR čili 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, hlavně v oblasti poskytování osobních údajů před, uzavřením pracovního poměru, v době jeho trvání a jak je s nimi nakládáno při jeho skončení. Práce je rozdělena na teoretickou a praktickou část. Teoretická část práce vymezuje základní pojmy, dále specifika uvedených ustanovení. Empirická část práce analyzuje současný stav dodržení a plnění ustanovení zmiňovaného zákona ve vybrané společnosti. V závěrečné části práce pak autor, na základě získaných informací a osobních zkušeností z provádění konkrétních ustanovení zmiňovaného zákona, objasňuje zásadní postupy a řešení, která provází aplikaci těchto zákonných požadavků v reálném fungování a chodu výrobní společnosti. Společnost osobní údaje zpracovává, a proto je dle Nařízení EU 2016/679 (dále je „GDPR“) správcem osobních údajů. Interní směrnici si stanovuje práva a povinnosti zaměstnanců společnosti a ostatních fyzických osob a fyzických osob podnikajících při veškerém zpracování osobních údajů, a to jak při ručním, tak automatizovaném zpracování. Ke zpracování osobních údajů výše uvedených subjektů údajů dokládá nutný souhlas jednotlivých fyzických osob, ledaže jsou údaje zpracovávány v souladu s článkem 6 odst. 1 písm. b), písm. c) či písm. f) Obecného nařízení GDPR, tedy z důvodu plnění smlouvy, plnění právní povinnosti nebo oprávněného zájmu.

ABSTRACT

JANDOVÁ, O. *Juridical Aspects of the Protection of Personal Data in the Manufacturing Company: Bachelor Thesis*. České Budějovice: The College of European and Regional Studies, 2018. 78 p. Supervisor: Mgr. et Bc. Josef Kříha.

Keywords: personal data, protection of personal data, data subject, controller and processor of personal data

The Bachelor Thesis (hereinafter referred to as „**thesis**“) has the ambitions to clarify the application of individual provisions of the currently effective Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts, as amended, by means of the form of the theoretical – praxeological insight. The thesis deals with the protection of personal data and obligations which are consequent upon this, from the perspective of so called GDPR, i.e. Regulation No. 2016/679 of the European Parliament and the Council (EU), on the protection of natural persons with regard to processing of personal data and on free movement of such data, in particular in the field of the provision of personal data prior to the conclusion of a fixed-term employment relationship, within its duration and treatment of data at the termination of the employment relationship. The thesis is divided into the theoretical and practical part. The theoretical part of the thesis defines the basic concepts as well as the specifics of the mentioned provisions. The empirical part of the thesis analyzes the current state of observance and fulfilment of the provisions of the mentioned law in the selected company. The author, based on the information and personal experience gained from the implementation of the specific provisions of the mentioned law, explains the essential procedures and solutions that accompany the application of these legal requirements in real functioning and running of the manufacturing company in the final part of the thesis. The company processes the personal data and therefore according to EU Regulation 2016/679 (hereinafter referred to „GDPR“) is the controller of personal data. By means of the Internal Directive, the company defines the rights and obligations of the employees and the other natural persons and the natural persons operating in all processing of personal data, both in manual and automated one. In order to process the

personal data of the above mentioned data subjects, the company shall require the consent of individual natural persons unless the data is processed in accordance with Article 6 (1) point (b), point (c) or point (f) of the General Regulation of GDPR, i.e. due to the performance of the contract, fulfilment of the legal obligation or a legitimate interest.

Obsah

Úvod.....	8
1 Cíl a metodika bakalářské práce	10
2 Základní právní úprava ochrany osobních údajů	11
3 Základní pojmy používané v oblasti ochrany osobních údajů	15
3.1 Základní pojmosloví a východiska.....	15
3.2 Základní pojmy.....	15
4 Personalistika	19
4.1 Zpracování osobních údajů před uzavřením pracovního poměru	19
4.2 zpracování osobních údajů za trvání pracovního poměru	25
4.3 Monitoring zaměstnanců	28
4.3.1 Kamery na pracovišti	32
4.3.2 Monitorování služebních telefonů	35
4.3.3 Monitorování služebních automobilů	36
4.3.4 Monitorování e-mailové pošty zaměstnanců	38
4.4 Fotografie v osobním spisu zaměstnance z hledisky zákona o ochraně osobních údajů 40	
4.5 Poskytování osobních údajů o zaměstnancích	46
4.6 Předávání osobních údajů do zahraničí	51
4.7 Zpracování osobních údajů po ukončení pracovního poměru.....	56
5 Empirická část.....	58
5.1 Analýza informací	58
5.1.1 Hypotézy	61
5.1.2 Vyhodnocení rozhovorů.....	61
Seznam použitých zdrojů	73
Seznam zkratk	76
Seznam tabulek a grafů	77
Přílohy	78

Úvod

Soukromí je pojem, který je znám snad každému a který je i hojně používán v různých souvislostech. Každý z nás si musí uvědomit, že soukromí je chráněno, že máme právo se ochrany domáhat a že se ochrany také můžeme dobrat, respektive jsou cesty a prostředky jak toho, kdo nám do našich práv zasahuje, nějak postihnout nebo donutit, aby se zásahy přestal.

Soukromí, jakožto osobnostní kategorie již dávno přesáhla kdysi zažitou teorii „čtyř stěn“, která jakoby tuto oblast vztahovala jen do omezeného a jiným nepřístupného prostoru, a dokonce ve fyzickém smyslu. Ač tedy dnes zákony *expressis verbis* neobsahují definici typu „soukromí je.....“, právní věda zahrnuje řadu aspektů, jakožto předmětu své ochrany.

Ústavní soud v rámci svého meritorního rozhodování například uvedl¹, že *„právo na ochranu soukromého života je nezadatelným právem fyzické osoby“*. V právní teorii se lze setkat s přístupem, dle něhož lze právo na ochranu osobního soukromí vymezit jako právo fyzické osoby rozhodnout podle vlastního uvážení zda, popřípadě v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným (pozitivní složka práva) a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob rovným právním postavením (negativní složky práva). Přílišná akcentace pozitivní složky práva na ochranu soukromého života vede k neadekvátnímu zúžení ochrany pouze, na to, aby skutečnosti soukromého života fyzické osoby nebyly zpřístupňovány veřejnosti bez jejího souhlasu či bez důvodu uznávaného zákonem, a tak nebyla narušována integrita vnitřní sféry, která je pro příznivý rozvoj osobnosti nezbytná. O typický případ porušení práva na osobní soukromí jde především tehdy, jestliže někdo neoprávněně získává vědomosti o skutečnostech soukromého života jiné osoby, ale také tehdy, jestliže tyto skutečnosti rozšiřuje. Ústavní soud nesdílí toto zúžené pojetí, které je odrazem konstrukce zakotvené v občanském zákoníku č. 89/2012 Sb., ve znění pozdějších předpisů, a poukazuje na dosavadní rozhodnutí Evropské komise a Evropského soudu pro lidská práva týkající se interpretace a aplikace čl. 8 odst. 1 Úmluvy, z níž (v souvislosti s projednávanou věcí) zdůrazňuje především myšlenku, že respektování soukromého života musí zahrnovat do určité míry právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi (této judikatury se také dovolává stěžovatelka). Součástí soukromého života je též rodinný život zahrnující i vztahy mezi blízkými příbuznými, když součástí rodinného života jsou, zahrnuje nejen sociální a morální vztahy, ale také zájmy materiální povahy (například vyživovací povinnost).

Respektování takto pojatého rodinného života zahrnuje závazek státu jednat způsobem umožňujícím „normální rozvoj těchto vztahů“. Je tedy zjevné, že soukromí, a i na ústavní rovině, je chápáno velmi široce s přesahem do reálných životních situací a

¹ Nález Ústavního soudu II. ÚS 517/99 zdroj: Systém ASPI – stav k 28. 5. 2015 do částky 53/2015 Sb. A 21/2015 Sb. m. s. – RA717 JUD32025CZ – JUD32025CZ – II ÚS 517/99 - Nedotknutelnost osoby a soukromí – poslední stav textu

mezilidských vztahů. Právo na ochranu soukromí patří mezi základní lidská práva, garantovaná Listinou základních práv a svobod² v Čl. 10³.

Reálným projevem takto garantované ochrany je její průmět do práva občanského, práva trestního, a i práva správního. Z jiného pohledu ochrana soukromí tak nachází výraz jak v oborech práva soukromého, tak i práva veřejného. Soukromoprávní ochranu garantuje Občanský zákoník v ustanovení § 84 až § 90. U

stanovení § 86 například postuluje, že „nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořizené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy“.

Zásahem do soukromí může být i spáchán trestný čin. Trestní zákoník obsahuje i několik skutkových podstat, které sankcionují zasahování do soukromí, souhrnně označované jako „trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství“. Jde o trestný čin neoprávněného nakládání s osobními údaji (§ 180), poškození cizích práv (§181), porušení tajemství doručovaných zpráv (§ 182), porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183) a konečně pomluvy (§ 184), přičemž tresty mohou být i velmi vysoké, u kvalifikovaných skutkových podstat až i 10 let odnětí svobody. Za třetí pilíř oné ústavní garance práva na soukromí, může být považována veřejnoprávní ochrana, specifikovaná v zákoně o ochraně osobních údajů. Ten hned v § 1 stanoví, že „tento zákon v souladu s právem Evropské unie, mezinárodními smlouvami, kterými je Česká republika vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států“.

Posledně uvedený zákon je zákonem obecným, který svými principy musí postihnout vlastně všechny oblasti, kdy jsou osobní údaje zpracovávány. Těch oblastí je celá řada, obecně a s jistou nadsázkou se dá i říci, že kde se v právních předpisech, právních vztazích, a nejen v nich, hovoří o lidech, jsou nějakým způsobem zpracovány informace o nich, a i nějak se s informacemi nakládá. Zaměstnávání lidí a pracovní právní vztahy jsou samozřejmě také o lidech a informacích o nich. Základní předpis pracovního práva, Zákoník práce, je předpisem práva svým charakterem soukromého. Jeho aplikace na pozadí zákona o ochraně osobních údajů pak staví před běžného uživatele, tedy zaměstnance i zaměstnavatele, řadu aplikačních problémů.

² Pospíšil, I., Langášek, T., Šimíček, V., Wagnerová, E., a kol., *Listina základních práv a svobod.*, Praha: 2012.

³ (1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě

1 Cíl a metodika bakalářské práce

Hlavním cílem práce je posouzení aplikace ustanovení zákona na ochranu osobních údajů v reálném chodu výrobní společnosti s nadnárodní účastí, kde dochází ke sběru dat od zaměstnanců vědomého i nevědomého a jak je s nimi nakládáno dál.

Vedlejším cílem práce je provedení zjišťovacího procesu, kdy a jak je pracovník informován, jakým způsobem je s informacemi, které společnosti poskytl, nakládáno. Z tohoto důvodu bylo provedeno vyhodnocení aplikace ustanovení zákona na ochranu osobních údajů.

Zkoumaná oblast je zvolena především na základě vlastní zkušenosti, neboť aplikace ustanovení zákona na ochranu osobních údajů spadá pod personální oddělení a je autorovi velice dobře známa, pracuje v této sféře. Bezpečné zpracování osobních údajů se autora tedy bezprostředně dotýká, a to nejen jako zaměstnance, ale i jako osoby zodpovědné za řádné vedení agendy.

Nedílnou součástí této práce je uvedení legislativy, podle které se musí veškeré zpracování osobních a citlivých údajů řídit, se zaměřením na ochranu osobních údajů, a soukromí, což již je a v budoucnu bude často řešené téma z důvodu jejich omezování. Pro danou tematiku jsem se rozhodla, protože se domnívám, že se jedná o poměrně aktuální téma, které se týká nás všech.

K získání výsledků byla aplikována metoda polo-strukturovaných rozhovorů s pracovníky společnosti, kteří se zabývají správou dat (členové personálního oddělení a oddělení IT) a druhá část zahrnovala použití metody polo-strukturovaných rozhovorů s pracovníky společnosti, tedy těmi, co poskytují tyto osobní údaje.

2 Základní právní úprava ochrany osobních údajů

Mezinárodní zkušenosti postupně ukazovaly, že ochranu osobních údajů není možné řešit výlučně na národní úrovni. Rostoucí objem přenášených osobních údajů mezi státy, vytváření mezinárodních databank, zvyšující se pohyb lidí bez ohledu na hranice států, rostoucí mezinárodní spolupráce v oblastech vědy a výzkumu kladly nové požadavky na mezinárodní koordinaci při ochraně osobních informací. Bylo nutno sjednotit principy ochrany osobních dat a jednotně pojmenovat rizika plynoucí z jejich volného přenosu. Z těchto potřeb vycházela také Organizace pro ekonomickou spolupráci a rozvoj (OECD), která již v roce 1969 vypracovala studii o přenosu dat přes hranice států pro potřebu veřejného sektoru a 23. září 1980 vydala Průvodce o ochraně soukromí a o přenosu osobních dat přes hranice států (Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data). Při přípravě tohoto dokumentu spolupracovala OECD s Radou Evropy, která v té době již měla zpracovaný návrh úmluvy o soukromí (Convention on Privacy). V tomto dokumentu byly poprvé definovány pojmy, které byly následně používány ve všech dalších právních předpisech. Byl definován pojem „správce“ (data controller) jako subjekt, který musí ze zákona nést základní odpovědnost za aktivity týkající se zpracování osobních údajů. Rovněž byly definovány pojmy jako „subjekt údajů“, „osobní údaje“, přenos přes hranice a další. Od roku 1980 se tak tyto pojmy začaly všeobecně používat nejen v právních předpisech jednotlivých členských států OECD, ale také v mezinárodním právu.⁴

Tento vývoj na mezinárodní scéně nezadržitelně směřoval k roku 1981, kdy došlo k částečnému ujednacení roztržité právní úpravy na evropském poli ochrany osobních údajů, a to vznikem Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. Tato úmluva zaručuje na území každé smluvní strany každé fyzické osobě, ať je jakékoli národnosti nebo pobývá kdekoli, úctu k jejím právům, základním svobodám a zejména k jejímu právu na soukromý život se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují. Tato úmluva zavedla do mezinárodního práva zejména zásady ochrany osobních údajů, které pak převzaly jednotlivé státy. Jedná se o zásady legitimacy zpracování, nezbytnosti časového omezení, potřebnosti a přiměřenosti, průhlednosti, bezpečnosti, práva přístupu k informacím, nezávislého dozoru a mnoho dalších. Ani tato úmluva však nezůstala do dnešních dnů ve svém původním rozsahu, dvacet let po svém schválení byla roku 2001

⁴ Bartík, V., Janečková, E.: Zákon o ochraně osobních údajů. Komentář. Praha 2010, s. 26.

rozšířena Dodatkovým protokolem o orgánech dozoru a toku údajů přes hranice. V této rozšířené podobě se úmluva dodnes hojně využívá.⁵

Tato Úmluva je velmi důležitá i ve vztahu k povinnosti žádat Úřad pro ochranu osobních údajů o povolení k předání osobních údajů do zahraničí. Úmluva č. 108 ve svém článku 3 odst. 2 písm. c) stanoví, že kterýkoliv stát může při podpisu nebo uložení ratifikační listiny, při přijetí, při schválení, přistoupení nebo kdykoliv později sdělit prohlášením zaslaným generálnímu tajemníkovi Rady Evropy, že uplatní tuto úmluvu rovněž na soubory osobních údajů, které se nezpracovávají automatizovaně. Česká republika toto prohlášení učinila současně s ratifikací Dodatkového protokolu k uvedené Úmluvě č. 108 dne 24. září 2003.

Pro přeoslání osobních údajů do státu, které ratifikovaly Úmluvu č. 108, to znamená, že ze strany České republiky se tato Úmluva vztahuje jak na automatizované, tak i neautomatizované zpracování osobních údajů a pokud je naplněn její článek 12 odst. 2⁶, platí pro oba typy těchto datových souborů, že smluvní strana nemůže pouze z důvodu ochrany soukromého života zapovědět nebo podrobit zvláštnímu povolení tok osobních údajů směřující na území druhé smluvní strany. Rovněž § 27 odst. 2 zákona 4. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“) připouští výjimky z povinnosti žádat Úřad pro ochranu osobních údajů o povolení k předání osobních údajů do zahraničí, pokud zákaz omezování volného pohybu osobních údajů vyplývá z mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas, a kterou je Česká republika vázána. Není pochyb o tom, že zmiňované ustanovení zákona se týká i Úmluvy č. 108.

Z výše uvedeného tedy vyplývá, že pro předání osobních údajů do států, které ratifikovaly Úmluvy č. 108⁷, není nutné žádat o povolení ve smyslu § 27 odst. 4 zákona o ochraně osobních údajů a ani Úřad pro ochranu osobních údajů není oprávněn zahajovat řízení o povolení k předání, neboť by se v tomto případě jednalo o úkon, který

⁵ Janečková, E., Bartík, V., Ochrana osobních údajů v pracovním právu, Wolters Kluwer ČR, Praha 2016, s. 12

⁶ Smluvní strana nemůže pouze z důvodu ochrany soukromého života zapovědět nebo podrobit zvláštnímu povolení tok osobních údajů směřujících na území druhé smluvní strany.

⁷ Vedle členských států Evropské unie podepsaly a ratifikovaly Úmluvu č. 108 např. tyto státy: Albánie, Bosna a Hercegovina, Černá Hora, Gruzie, Chorvatsko, Island, Lichtenštejnsko, Makedonie, Norsko, Srbsko, Švýcarsko. Dodatkový protokol k Úmluvě č. 108 podepsaly a ratifikovaly např. tyto státy: Albánie, Česká republika, Francie, Kypr, Litva, Lucembursko, Maďarsko, Německo, Nizozemí, Polsko, Slovensko, Švédsko.

by byl v rozporu s cíli zmiňované mezinárodní smlouvy i se zákonem o ochraně osobních údajů⁸.

Po ratifikaci této Úmluvy následovalo přijetí zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl prvním uceleným právním předpisem v oblasti ochrany osobních údajů. Poskytoval definice některých termínů, jako například osobní údaj, informační systém, provozovatel informačního systému, dotčený subjekt, zveřejněná informace a další. Zákon také určoval, jakým způsobem je dovoleno získávat a pak dále zpracovávat jednotlivé osobní údaje a jak je zabezpečit. Problém tohoto zákona však byla jeho bezzubost, postrádal naprosto sankční ustanovení ani nestanovil žádný dozorový orgán, a tak se stal spíše proklamací bez valného praktického účinku. Tento nedostatek napravil až současný zákon o ochraně osobních údajů⁹. S jistou mírou nadsázky lze tedy konstatovat, že šlo spíše o předpis obsoletní, protože v podstatě nikdy nebyl v praxi realizován.

Vzhledem k tomuto stavu nebyl český právní řád, kam byl zmíněný zákon o ochraně osobních údajů zařazen, kompatibilní s právem Evropské unie, na jejíž půdě byla přijata zvláštní Směrnice Evropského parlamentu a rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů, která ukládala členským státům, aby ji promítly do tří let do svých právních řádů. Svoje zákony s ní musely samozřejmě harmonizovat i státy, které se chtěly stát členy Evropské unie. Jedním z nejvýznamnějších přínosů této směrnice, kromě výrazného příspěvku k harmonizaci národních předpisů, je deklarace faktu, že státy nesmějí omezit ani zakázat volný pohyb osobních údajů mezi členskými státy z důvodu ochrany podle ustanovení této směrnice.

Směrnice vychází v podstatě z Úmluvy, ale výrazně ji rozšiřuje a prohlubuje. Stanovuje požadavky na technickou bezpečnost zpracování dat, ukládá povinnost oznamovat zpracování osobních údajů a mít souhlas dotčené osoby se zpracováním, požaduje vytvoření nezávislého orgánu dozoru, rozšiřuje ochranu osobních údajů také na neautomatizovaně zpracovávané údaje a údaje přenášené mimo Evropskou unii, definuje zvláštní kategorii údajů, tzv. citlivé údaje. Řeší problematiku ochrany

⁸ *Předávání osobních údajů do zahraničí / Aplikace Úmluvy Rady Evropy č. 108 ve vztahu k povinnosti žádat Úřad o povolení k předání osobních údajů do zahraničí.*: [online]. Praha: UOOU, 2014 [cit. 2014 únor]. Dostupné z WWW: <<http://uoou.cz/k-problemum-z-praxe/ds-1651/archiv=1633>>.

⁹ Janečková, E., Bartík, V., *Ochrana osobních údajů v pracovním právu*, Wolters Kluwer ČR Praha, 2016, str. 13.

fyzických osob (nevztahuje se tedy na ochranu právnických osob v této oblasti) v souvislosti se zpracováním osobních údajů. Hned v úvodu této směrnice je uvedeno, že při zpracování osobních údajů musí být dodrženy základní svobody a práva osob, zejména pak právo na soukromí.

Cílem této směrnice je zajistit vysokou úroveň ochrany osobních údajů ve všech členských státech Unie, zajistit volný pohyb informací a informačních služeb mezi členskými státy (zejména z důvodu stále se rozvíjejícího vnitřního trhu), stanovit společný rámec pro práci s osobními údaji a jejich ochranu na území Evropské unie a sladit národní legislativu v této oblasti platnou na území jednotlivých států (členské státy si mohou v národních předpisech upřesnit obecné podmínky a zákonitosti zpracování osobních údajů. Zásady ochrany se musí vztahovat na veškeré zpracování osobních údajů kteroukoliv osobou, jejíž činnosti spadají do oblasti působnosti práva EU, musí se vztahovat na veškeré informace týkající se identifikované nebo identifikovatelné osoby a vztahují se i na zvukové a obrazové údaje týkající se fyzických osob.

Velký důraz je při ochraně subjektů kladen zejména na nutnost získání souhlasu subjektu se zpracováním osobních údajů, zákonnost zpracování, nutnost oznámení zpracovávání, právo subjektu osobních údajů na získání informací a opravu osobních údajů, bezpečnost zpracování a omezený sběr. Od 1. ledna 1999 se veškeré akty Evropských společenství o ochraně fyzických osob při zpracování osobních údajů a při volném pohybu takových údajů uplatňují vůči institucím založeným Amsterodamskou smlouvou. Tak se ochrana osobních dat stala součástí smluv o založení Evropského společenství, a tak i součástí primárního práva¹⁰.

Všechny tyto mezinárodní dokumenty vedly k přijetí zákona o ochraně osobních údajů tak, jak ho známe dnes. Zákon byl přijat v roce 2000 a od té doby byl již 23krát novelizován. Je nutné ještě dodat, že některé z novel nejsou dosud účinné.

¹⁰ Janečková, E., Bartík, V., Ochrana osobních údajů v pracovním právu, Wolters Kluwer ČR Praha, 2016, str. 14

3 Základní pojmosloví a východiska používaná v oblasti ochrany osobních údajů

3.1 Základní pojmosloví a východiska

S poukazem k aplikaci ustanovení § 4 zákona o ochraně osobních údajů lze vymezit základní pojmy a chápat pojem osobní údaj, neboť z pojmů a z jejich aplikace vycházejí v zákoně upravená práva a povinnosti těch, na které se zákon vztahuje. Nejprve je nutné ujistit se, že údaj, s nímž správce pracuje, je osobním údajem ve smyslu zákona o ochraně osobních údajů, zda s údajem prováděný proces je zpracováním tak, jak jej chápe zákon o ochraně osobních údajů atd., a teprve v případě kladné odpovědi na tyto otázky se správce zabývá dalšími ustanoveními zákona o ochraně osobních údajů, jež mu ukládají povinnosti a dávají práva. Vymezeny jsou všechny základní pojmy ve smyslu jejich hmotného obsahu (např. osobní údaj) a také pojmy, které lze označit za „popis procesu“ (např. zpracování). Pojmy obecně vycházejí z mezinárodních dokumentů, které byly jednak ideovým vzorem a jednak pramenem práva, na jejichž základě byl zákon koncipován a později také v různém rozsahu novelizován¹¹.

3.2 Základní pojmy

Osobní údaj: jakákoli informace o identifikované nebo identifikovatelné fyzické osobě (subjekt údajů), identifikovatelnou fyzickou osobou je osoba, kterou lze přímo nebo nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její tělesné, fyziologické, psychické, ekonomické, kulturní nebo sociální identity. Osobním údajem může být například jméno a příjmení, datum narození, adresa, číslo bankovního účtu, informace o vzdělání a praxi, telefonní číslo, adresa elektronické pošty, záznam z kamerového systému atd.

Citlivý údaj: osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v oborech, náboženství nebo filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě.

¹¹ Janečková, E., Bartík, V., Ochrana osobních údajů v pracovním právu, Wolters Kluwer ČR Praha, 2016, str. 15

Anonymní údaj: jímž je takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů. Definicí pojmu anonymní údaj je třeba chápat kontextuálně ve vztahu k jiným definicím, zejména však k pojmu osobní údaj. Již z definice a výše uvedeného vztahu k pojmu osobní údaj je zřejmé, že bude-li někdo zpracovávat informace, které jsou anonymní již na samém počátku sběru takových informací, které nelze vztáhnout ke konkrétní fyzické osobě, a tato osoba není ani ze shromážděných informací určitelná, nebude se vůbec jednat o aktivity, na které by bylo možno vztáhnout zákon o ochraně osobních údajů, a to proto, že se nebude jednat o osobní údaje, ve smyslu definice tohoto zákona.¹²

Pseudonymizace: je zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.

Zveřejněný osobní údaj: který zákon definuje jako osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

Subjekt údajů: fyzická osoba, k níž se osobní údaje vztahují, jednoduše řečeno, jste to Vy.

Omezení zpracování: je označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu.

Evidence: je jakýkoliv strukturovaný soubor osobních údajů přípustných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.

Profilování: je jakákoliv forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se ke konkrétní fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejich

¹²*Ochrana osobních údajů na pracovišti*, [online]. Praha, UOOU, 2014. Dostupné z WWW: <http://uoou.cz/assets/File.ashx?id_org=200144id_dokumenty=12691>.

pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

Zpracování osobních údajů: jakákoli operace nebo soustava s osobními údaji, ať už automatizovanými nebo jinými prostředky, jako je shromažďování, ukládání na nosiče informací, uchovávání, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, třídění nebo kombinování, blokování a likvidace. Dokonce jedna samostatná operace (například shromažďování) je zpracování osobních údajů.¹³

Správce údajů: každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj, nebo subjekt, který je povinen zpracovat určité osobní údaje na základě zvláštního zákona, například zaměstnavatel, jehož povinností je zpracovávat řadu kategorií údajů o zaměstnancích pro potřeby sociálního a zdravotního pojištění, daňové kontroly aj.

Zpracovatel: každý subjekt jiný než správce, který zpracovává osobní údaje pro správce, například zprostředkovatelna práce při hledání zaměstnance pro určitou práci, externí firma zpracovávající mzdové účetnictví apod.

Třetí stranou: je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.

Souhlas: je svobodný, výslovný a vědomý (informovaný) projev vůle, kterým subjekt údajů dává svolení se zpracováním osobních údajů, jež se ho týkají.

Příjemce: je každý subjekt, kterému jsou osobní údaje zpřístupněny, za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g).

Porušení zabezpečení osobních údajů: je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovaných osobních údajů.

¹³*Ochrana osobních údajů na pracovišti*, [online]. Praha, UOOU, 2014. Dostupné z WWW: <http://uouu.cz/assets/File.ashx?id_org=200144id_dokumenty=12691>.

Genetický údaj: je osobní údaj týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené osoby.

Biometrický údaj: je osobní údaj vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, např. zobrazení obličeje nebo daktyloskopické údaje.

Údaj o zdravotním stavu: je osobní údaj týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.¹⁴

Zástupce: je jakákoli fyzická nebo právnická osoba usazená v Evropské unii, která je správcem nebo zpracovatelem určena písemně, aby správce nebo zpracovatele zastupovala.

Podnik: je jakákoliv fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost.

Skupina podniků: je skupina zahrnující řídicí podnik a jím řízené podniky.

Závazná podniková pravidla: je koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost.

Dozorový úřad: je nezávislý orgán veřejné moci zřízený členským státem.

Mezinárodní předávání dat: pohyb osobních údajů uvnitř Evropské unie (EU), Evropského hospodářského prostoru (EHP) nebo jakýkoli přenos osobních údajů do třetích zemí. V EU a EHP nesmí být tento pohyb omezen a není ani předmětem udělení souhlasu ze strany orgánů ochrany osobních údajů. Do třetích zemí mohou být údaje předávány jen po splnění zvláštních podmínek.

¹⁴*Ochrana osobních údajů na pracovišti*, [online]. Praha, UOOU, 2014. Dostupné z WWW: <http://uoou.cz/assets/File.ashx?id_org=200144id_dokumenty=12691>.

Orgán ochrany osobních údajů: je nezávislý úřad, který provádí dozor nad plněním povinností stanovených zákonem pro ochranu osobních údajů, přijímá a vyřizuje podněty a stížnosti ve věci porušení zákona při zpracování osobních údajů a provádí osvětovou činnost.¹⁵

4 Personalistika

Personalistika bývá obecně charakterizována jako činnost, která se zaměřuje na získávání pracovníků a práce s nimi. V širším slova smyslu je pak činností, kterou vykonává prakticky každý zaměstnavatel, který má či hodlá mít zaměstnance, a zahrnuje v sobě zejména plnění zákonných povinností, jež zaměstnavatelům ukládají zvláštní právní předpisy, ale také činnosti, které jsou v zájmu samotného zaměstnavatele na základě jeho vlastního rozhodnutí a týkají se jeho zaměstnanců. Vzhledem k tomu, že není myslitelné, aby se personální práce obešla bez údajů osob, zaměstnanců, jichž se personální práce týká, bude se v každém případě jednat o zpracování osobních údajů a na tato zpracování bude dopadat také zákon o ochraně osobních údajů. Rozdíl bude jen v tom, v jakém režimu, respektive jaká ustanovení zákona o ochraně osobních údajů budou dotčena a jaká práva a jaké povinnosti budou stíhat zaměstnavatele, a tedy jakými ustanoveními uvedeného zákona se budou jednotlivá zpracování řídit.

Z hlediska časové posloupnosti lze zpracování osobních údajů rozdělit do tří základních částí. Zpracování osobních údajů před uzavřením pracovního nebo obdobného poměru, zpracování v jeho průběhu a konečně po jeho ukončení¹⁶.

4.1 Zpracování osobních údajů před uzavřením pracovního poměru

V personálním oddělení se shromažďují požadavky na přijetí nového pracovníka. Personalista podle toho, o jakou pracovní pozici se jedná, zvolí vhodnou formu nábory. Jde o vlastní personální zdroje uvnitř společnosti nebo o zdroje z trhu práce a zaměstnanosti. Zde je jedno, zda se bude jednat o zprostředkování práce přes

¹⁵*Ochrana osobních údajů na pracovišti*, [online]. Praha, UOOU, 2014. Dostupné z WWW: <http://uoou.cz/assets/File.ashx?id_org=200144id_dokumenty=12691>.

¹⁶ Bartík, V., Janečková E., *Ochrana osobních údajů v aplikační praxi (vybrané problémy)*. , Praha 2016, str. 136

lokální Úřad práce nebo spolupráce s personální agenturou, která doporučí vhodného kandidáta.

Je tedy zřejmé, že správce (zaměstnavatel) je povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění určeného cíle. Splnění této povinnosti bude tedy vyžadovat přesné vymezení rozsahu konkrétních osobních údajů, které budou v daném případě k naplnění určeného cíle skutečně potřebné. Je tak třeba o každém osobním údaji rozhodnout, zda je či není pro daný účel nezbytný. Zvolí-li si správce nějaký rozsah osobních údajů, které hodlá zpracovávat, měl by být schopen u každého jednotlivého údaje odpovědět na otázku, proč je daného údaje třeba pro dosažení určeného úkolu. Cílem je dospět do stavu, kdy účelu zpracovávání bude dosaženo s použitím co nejmenší skupiny osobních údajů. Ty zbylé by měl správce bez zbytečného odkladu zlikvidovat, nebo je vůbec neshromažďovat.

Zákoník práce sice, na rozdíl od staré právní úpravy, věnuje pozornost postupu zaměstnavatelů před vznikem pracovního poměru, když v § 30¹⁷ stanoví, že 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. Předpoklady kladené zvláštními právními předpisy na fyzickou osobu jako zaměstnance tím nejsou dotčeny, a také, že zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy. Jak vidno, ani současná právní úprava v zákoníku práce není příliš konkrétní, což na druhou stranu nemusí být na škodu věci z hlediska ochrany osobních údajů. Stále platí limity stanovené zákonem o ochraně osobních údajů a je tedy jen otázkou správné interpretace a aplikace jak zákona o ochraně osobních údajů, tak zákoníku práce a v neposlední řadě i zákona o zaměstnanosti. Správnou interpretací a aplikací všech tří zákonů ve vzájemných souvislostech pak lze dosáhnout natolik vyváženého shromažďování a následného dalšího zpracování osobních údajů, že bude nejen

¹⁷Hloušková, P., Hofmanová, E., Knebl P., Roučková, D., Schmied, Z., Schweiner, P., Tomandlová, L., *Zákoník práce prováděcí nařízení vláda a další související předpisy k 1. 2. 2018.*, Praha: ANAG, 2018.

chráněno soukromí uchazečů o zaměstnání, ale také zaměstnavatelé budou mít dost informací pro to, aby mohli pracovní místo obsadit vhodným kandidátem.¹⁸

Základní hmotněprávní úpravu vztahů mezi fyzickou osobou, subjektem údajů a potencionálním zaměstnavatelem z hlediska práva pracovního představuje zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (dále jen „zákon o zaměstnanosti“), a zákoník práce. Dlužno předeslat, že takzvané prepracovní vztahy nebyly do přijetí zákona o zaměstnanosti upraveny vůbec, což činilo z hlediska ochrany osobních údajů a zpracování těchto údajů výkladové a aplikační problémy. Vzhledem k absenci základní právní úpravy činily problémy zejména takové záležitosti jako byl rozsah osobních údajů vyžadovaný potencionálními zaměstnavateli po uchazečích o zaměstnání, stejně tak jako údaje požadované personálními agenturami zejména tehdy, pokud tyto agentury byly správci osobních údajů. Těmi byly za situace, kdy samy aktivně působily na trhu práce, tedy shromažďovaly osobní údaje uchazečů o práci bez zakázky nějakého konkrétního zaměstnavatele. Problém byl zejména v aplikaci ustanovení § 5 odst. 1 písm. d) zákona o ochraně osobních údajů neboli povinnosti shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Tento účel byl deklarován velmi obecně, respektive široce tak, že se jednalo o shromáždění osobních údajů pro to, aby takové agentury mohly u nich registrované klienty, uchazeče o zaměstnání, volně nabízet na trhu práce. Jinak řečeno, vyhledávaly vhodné zaměstnavatele podle údajů, které získaly od svých klientů. Tyto údaje však byly shromažďovány ve značném rozsahu, a to včetně informací, které prakticky neměly vztah k potencionálnímu zaměstnání. Tak byly například shromažďovány i informace o majetkových poměrech klientů, pokud se týkaly formy bydlení (vlastní, nájemní, podnájemní), o rodinných poměrech, a dokonce i informace o uvažovaných sňatcích, plánovaném počtu dětí a podobně. Tehdy platné znění zákona o ochraně osobních údajů tuto praxi do jisté míry umožňovalo. Personální agentury bezpochyby zpracovávaly osobní údaje na základě souhlasu subjektů údajů. Ustanovení § 5 odst. 4 zákona o ochraně osobních údajů v tehdy platném znění (do 25. 7. 2004) bylo konstruováno jinak, než je tomu v současné době, a pro souhlas stanovovalo jeho rámeček tak, že „ze souhlasu musí být patrné, v jakém rozsahu je poskytován, komu a k jakému účelu, na jaké období a kdo jej poskytuje. Souhlas může být kdykoliv odvolán, pokud se subjekt údajů se

¹⁸ Bartík, V., Janečková, E.: Ochrana osobních údajů v aplikační praxi. Praha 2012, s. 155.

správcem výslovně nedohodne jinak. Tento souhlas musí správce prokázat po dobu zpracování osobních údajů, k jejichž zpracování byl dán souhlas.“ Takovým souhlasem personální agentury vesměs disponovaly, i když o „dobrovolnosti“ udělení takového souhlasu byly vedeny značné polemiky.

Problém kvality souhlasu a jeho novou definici nakonec vyřešila novela zákona o ochraně osobních údajů (zákonem č. 439/2004 Sb.), která nově definovala souhlas v ustanovení § 4 písm. n) zákona o ochraně osobních údajů tak, že souhlasem subjektu údajů je svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů, a dále nově definovala jeho další parametry v ustanovení § 5 odst. 4 tak, že subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období a že souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování. Souhlas se zpracováním osobních údajů byl tedy jednoznačně jednostranný úkon, zcela v souladu s ustanoveními § 37 a § 39 starého občanského zákoníku, a tak bylo třeba jej vykládat a aplikovat. Dnes platný občanský zákoník obsahuje právní úpravu obdobnou, nicméně se stejným smyslem a cílem.

Z hlediska ochrany osobních údajů je důležité, že zákonem o zaměstnanosti jsou od počátku jeho účinnosti stanoveny rozsahy údajů (informací), které vůbec není přípustné v prepracovním procesu, tedy ve fázi výběru zaměstnanců, zjišťovat. V § 12 odst. 2 zákona o zaměstnanosti je výslovně stanoveno, že zaměstnavatel nesmí při výběru zaměstnanců vyžadovat informace týkající se národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení, sexuální orientace, není-li jejich vyžadování v souladu se zákonnými výjimkami¹⁹, dále informace, které odporují dobrým mravům, a osobní údaje, které neslouží k plnění povinností zaměstnavatele stanovených zvláštním právním předpisem. Na žádost uchazeče o zaměstnání je zaměstnavatel povinen prokázat potřebnost požadovaného osobního údaje. Je tedy zřejmé, že zákonodárce vyloučil takzvané citlivé osobní údaje podle tehdy platného znění § 4 písm. b) zákona o ochraně osobních údajů²⁰ s výjimkou údaje o trestné činnosti. Tato informace totiž může být v některých případech pro budoucího

¹⁹ § 4 zákona o zaměstnanosti

²⁰ Citlivým údajem je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů

zaměstnavatele relevantní. Pro tento údaj ovšem také bude platit povinnost zaměstnavatele prokázat jeho potřebnost. Bude se jednat zejména o případy, kdy je na některou z pracovních pozic stanoven zvláštním právním předpisem požadavek bezúhonnosti, který bývá sice definován hmotněprávní různě z hlediska „tolerance“ některých druhů trestné činnosti, nicméně stanoven je. V případě, že by informaci požadoval zaměstnavatel bez přímé opory ve zvláštním právním předpisu, nebude sice snaha o získání této informace v rozporu se zákonem o zaměstnanosti, může však být v rozporu s ustanovením § 5 odst. 1 písm. d) zákona o ochraně osobních údajů²¹. Tehdy platný zákoník práce vůbec žádnou právní úpravu prepracovních vztahů neobsahoval, a tak zákon o zaměstnanosti ve spojení se zákonem o ochraně osobních údajů obsahoval jediné limity, pokud šlo o rozsah osobních údajů, které mohl zaměstnavatel při náboru zaměstnanců požadovat. Z toho vyplývá, že rozsah informací (osobních údajů), které může zaměstnavatel požadovat po uchazečích o zaměstnání, je značně omezen a může se týkat toliko údajů, které bezprostředně souvisí s obsazovaným pracovním místem. Bude se jednat o základní identifikační údaje, jako jméno nebo jména, příjmení, adresa bydliště, datum narození²² (nikoliv však rodné číslo), informace o vzdělání a praxi, případně i informace o zvláštních předpokladech²³ nebo schopnostech, které mají vztah k obsazované pracovní pozici a běžné kontaktní údaje, jako číslo telefonu nebo e-mailová adresa.

Nyní platný zákoník práce sice, na rozdíl od staré právní úpravy, věnuje pozornost postupu zaměstnavatelů před vznikem pracovního poměru, když v § 30 stanoví, že 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. Předpoklady kladené zvláštními právními předpisy na fyzickou osobu jako zaměstnance tím nejsou dotčeny a také, že zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy. Jak vidno, ani současná právní úprava zákoníku práce není příliš konkrétní, což na druhou stranu nemusí být na závadu věci z hlediska ochrany osobních údajů. Stále platí limity stanovené zákonem o ochraně

²¹ Shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu.

²² Přitom se musí brát v úvahu i riziko diskriminace z hlediska věku.

²³ Například zákon č. 451/1991 Sb., kterým se stanoví některé další předpoklady pro výkon některých funkcí ve státních orgánech a organizacích, ve znění pozdějších předpisů.

osobních údajů a je tedy jen otázkou správné aplikace jak zákona o ochraně osobních údajů, tak zákoníku práce a v neposlední řadě také zákona o zaměstnanosti. Správnou aplikací všech tří zákonů ve vzájemných souvislostech pak lze dosáhnout natolik vyváženého shromažďování a následného dalšího zpracování osobních údajů, že bude nejen chráněno soukromí uchazečů o zaměstnání, ale také zaměstnavatelé budou mít dost informací pro to, aby mohli pracovní místo obsadit vhodným kandidátem.

V rámci postupu zaměstnavatelů před vznikem pracovního poměru dochází k systematickému zpracování osobních údajů uchazečů. Je třeba odpovědět na otázku, zda k takovému zpracování potřebuje zaměstnavatel, tedy správce osobních údajů, souhlas subjektu údajů, či tak může činit bez souhlasu. Odpovědi na tyto otázky dává ustanovení § 5 odst. 2 zákona o ochraně osobních údajů v návěti a písm. b), kde je uvedeno, že správce (tedy zaměstnavatel) může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat, jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů. V případě náboru zaměstnanců se jedná právě o takový případ. Obecně bývá pravidlem, že zaměstnavatel hledající nové pracovní síly dá tuto skutečnost najevo veřejným sdělením, nejčastěji v podobě nabídkového inzerátu, který bývá zveřejněn v denním tisku a také na různých specializovaných informačních stránkách internetu. Zveřejňovány bývají většinou pouze 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.

Výsledkem je více či méně rozsáhlá databáze, kterou tvoří zaslané dokumenty jednotlivých uchazečů o zaměstnání, která obsahuje osobní údaje jednoho každého z nich, ač vnitřní struktura jednotlivých dokumentů bude zpravidla různá, i když víceméně obdobná. Tento soubor osobních údajů uchazečů o zaměstnání splňuje kritéria definice podle § 4 písm. m) zákona o ochraně osobních údajů a je evidencí, která je dále zpracovávána za účelem výběru vhodného uchazeče, a konečným cílem a účelem zpracování je uzavření pracovní smlouvy s vybraným kandidátem. Je tedy zřejmé, že je naplněna litera ustanovení § 5 odst. 2 písm. b) zákona o ochraně osobních údajů, neboť se prakticky jedná o jednání o uzavření smlouvy, byť je toto jednání v pouhém zahajovacím stadiu. Není třeba, aby zaměstnavatel takové zpracovával s formalizovaným souhlasem subjektu údajů, uchazečů o zaměstnání.

Je přitom zřejmé, že uchazeči jsou seznámeni s účelem, k němuž poskytují své osobní údaje, a komu. Je jim znám i rozsah údajů, neboť na základě rámcové informace je poskytují sami o své vůli a v rozsahu často větším, než je požadováno. Mohou do značné míry také dovodit, na jak dlouhou dobu je poskytují (do doby, než bude vybrán vhodný uchazeč) a jsou s těmito skutečnostmi srozuměni.

4.2 Zpracování osobních údajů za trvání pracovního poměru

Je nepochybné, že v průběhu trvání pracovního poměru bude zaměstnavatel zpracovávat osobní údaje ve velkém rozsahu.

Údaje, které zaměstnavatel o zaměstnanci shromažďuje a dále zpracovává během trvání pracovního poměru, je možné rozdělit na ty, které o zaměstnanci shromažďovat musí, a na ty, které shromažďovat může.

Povinnost údaje shromažďovat je zaměstnavateli uložena prostřednictvím právních předpisů z oblasti sociálního zabezpečení, stejně tak jako prostřednictvím ustanovením právních předpisů z oblasti daňové. Řada povinností na vytvoření určitých souborů dat je zaměstnavateli uložena i přímo zákoníkem práce, stejně jako například zákonem o zaměstnanosti či speciálními sektorovými nebo oborovými předpisy upravujícími výkon určitých povolání nebo činností.

Vedle povinně shromažďovaných údajů zde existuje i řada údajů, které zaměstnavatel sice o zaměstnanci povinnost shromažďovat nemá, avšak jestliže uzná za vhodné a účelné provádět takové shromažďování dat, které je předdefinováno právním předpisem, svědčí mu pro něj právě na základě příslušného právního předpisu právní titul v podobě zákonné podmínky.

Poslední případ zpracování, respektive shromažďování osobních údajů zaměstnavatelem o zaměstnanci během trvání pracovního poměru, představuje předem nedefinované a ani zaměstnavateli nijak neuložené zpracování osobních údajů-zpracování, které zaměstnavatel provádí na základě vlastního rozhodnutí.

Čím delší pracovní poměr bude, tím více údajů bude zpracováváno a tím více otázek si zaměstnavatel musí klást. A podle současného vývoje by si podobné otázky měl klást i zaměstnanec.

Jednou ze značně frekventovaných otázek je, zda se zaměstnavatel musí registrovat u Úřadu pro ochranu osobních údajů pro to, že zpracovává osobní údaje svých zaměstnanců. Ustanovení § 16 odst. 1 zákona o ochraně osobních údajů stanoví, že ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracovávání podle tohoto zákona, s výjimkou zpracování uvedených v § 18, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováním osobních údajů. A právě ustanovení § 18 odst. 1 písm. b) zákona o ochraně osobních údajů je důležité pro pochopení možnosti zaměstnavatelů zpracovávat osobní údaje svých zaměstnanců a pochopení, zda mají zaměstnavatelé oznamovací povinnost plnit. Oznamovací povinnost podle § 16 zákona o ochraně osobních údajů a mimo jiné nevztahuje na zpracování osobních údajů, které správci ukládá zvláštní zákon, nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona. Znamená to, že zaměstnavatel (z hlediska zákona o ochraně osobních údajů správce osobních údajů) musí znát a aplikovat celou řadu právních předpisů, které mu ukládají spoustu povinností, a z nich plyne, že musí zpracovávat značné množství osobních údajů. Tyto zvláštní zákony také přímo či nepřímo určují, které konkrétní údaje, nebo chceme-li informace o zaměstnancích, zpracovávány být musí. Kromě základního předpisu pracovního práva, tedy zákoník práce, je třeba poukázat alespoň na zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, zákon č. 155/1995 Sb., o důchodovém pojištění, a jeho § 74 nebo 76, zákon č. 582/2004 Sb., o organizaci provádění sociálního zabezpečení, a ustanovení § 37, zákon č. 435/2004 Sb., o zaměstnanosti, a jeho § 80 až 83 (pojem vymezen v § 67 odst. 2), zákon č. 586/1992 Sb., o daních z příjmu, a mnohé další.

Oproti dříve platnému současnému zákoník práce dává právo zaměstnavateli vést osobní spis zaměstnance²⁴. Tento osobní spis však může obsahovat jen písemnosti, které jsou nezbytné pro výkon práce. Jedná se tak vlastně o obdobný limit, kterým zákon o ochraně osobních údajů stanoví správčům osobních údajů povinnost shromažďovat osobní údaje pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu, a to v § 5 odst. 1 písm. d) zákona o ochraně osobních údajů. Typicky se bude jednat o listiny, které tvoří „informační základnu“ zaměstnavatele o jeho zaměstnancích a které je zaměstnanec povinen zaměstnavateli poskytnout, a to právě pro plnění jeho zákonných povinností. Základní údaje bývají nejčastěji uvedeny v

²⁴Hloušková, P., Hofmanová, E., Knebl P., Roučková, D., Schmied, Z., Schweiner, P., Tomandlová, L., *Zákoník práce prováděcí nařízení vláda a další související předpisy k 1. 2. 2018.*, Praha: ANAG, 2018.

tzv. osobním dotazníku, který se vyplňuje většinou ještě před formálním uzavřením pracovního poměru podpisem pracovní smlouvy. Vzhledem k zákonným limitům uvedeným výše by měl takový dotazník, respektive jeho základní obsah, být u všech zaměstnavatelů prakticky stejný. Bude se jednat o základní identifikační údaje, tedy jméno a příjmení, adresu bydliště, informace o trestní bezúhonnosti zaměstnance, je-li takových údajů pro vykonávanou práci zapotřebí, údaj o provozování vlastní podnikatelské činnosti, druhu podnikání a výkonu jiné pravidelné výdělečné činnosti, pro některé zaměstnavatele je také nezbytné mít informace o členství zaměstnance v řídicích a kontrolních orgánech právnické osoby provozující podnikatelskou činnost, informace o zvláštních oprávněních nebo způsobilostech, jako je oprávnění k řízení motorových vozidel, vlastnictví zbrojního průkazu či způsobilost pracovat s utajovanými informacemi a získané bezpečnostní způsobilosti, pokud výše uvedené informace, které jsou bezpochyby osobními údaji, jsou nezbytné pro výkon zaměstnání. Součástí osobního spisu pak budou dokumenty, které pro zaměstnavatele osvědčují informace uvedené v osobním dotazníku, a dále dokumenty, které přímo souvisí se zaměstnaneckým poměrem. Bude se typicky jednat o druhopis pracovní smlouvy, platební výměr, kopie o dosaženém vzdělání a získaných zvláštních kvalifikacích apod.

Je samozřejmě možné, aby zaměstnavatel zpracovával i jiné osobní údaje, pokud je přesvědčen, že je k výkonu zaměstnaneckých funkcí potřebuje a tato potřeba vychází např. ze zvláštních sociálních programů, pravidel nadstandardních požitků stanovených vnitřními předpisy zaměstnavatele apod. V takovém případě se ovšem zpracování osobních údajů, které není zaměstnavateli uloženo zvláštními zákony, řídí obecným pravidlem stanoveným § 5 odst. 2 zákona o ochraně osobních údajů a takové údaje je možno zpracovávat jen se souhlasem zaměstnance. Existuje-li např. sociální program, který umožňuje zaměstnancům čerpat nějaké výhody i pro rodinné příslušníky, typicky se jedná o děti mladší 15 let, mají někteří zaměstnavatelé tendenci zjednodušovat si práci a vyžadují od svých zaměstnanců například kopii rodného listu dítěte. Tento požadavek jen zřídka bývá zaměstnancem odmítnut, a tak ve spisech jsou uloženy také veškeré informace, které rodný list obsahuje a které bezpochyby nesouvisí s poskytovaným benefitem. Jsou tak uchovávány, a tedy také zpracovávány osobní údaje osob, k jejichž zpracování obecně nemají zaměstnavatelé žádné oprávnění, když poskytnutí kopie rodného listu, pod podmínkou nemožnosti čerpání sociálních benefitů, nelze považovat za souhlas se zpracováním osobních údajů ve smyslu ustanovení § 4 písm. n) zákona o ochraně osobních údajů.

Pokud tedy zaměstnavatel zpracovává osobní údaje svých zaměstnanců pouze za účelem vedení personální a mzdové agendy, pro dodržení jeho právních povinností uložených zvláštními zákony, nemusí plnit oznamovací povinnost podle § 16 zákona o ochraně osobních údajů. Oznamovací povinnost podle § 16 tohoto zákona se na zaměstnavatele vztahuje pouze v tom případě, že zpracovává osobní údaje svých zaměstnanců i pro jiné účely, než je mu uloženo zvláštními zákony,²⁵ anebo zpracovává údaje, jejichž zpracování nevyplývá ze žádného právního předpisu a jejich zpracování je založeno na souhlasu zaměstnance. V takovém případě je třeba oznamovací povinnost podle § 16 zákona o ochraně osobních údajů splnit.²⁶

4.3 Monitoring zaměstnanců

Jednou z oblastí, která je v důsledku v minulosti zcela nevídaného rozvoje odposlouchávacích, kamerových a jiných podobných zařízení stále častěji veřejností v tomto smyslu přetřásána, je vyjma obecné problematiky ochrany soukromí člověka také ochrana soukromí zaměstnance při výkonu práce pro zaměstnavatele. Zatímco stávající právní úprava ochrany soukromí nedoznala za posledních padesát let žádných výrazných změn, informační a komunikační technologie, které umožňují toto právo narušit, naopak prošly změnami zcela zásadními, a to včetně jejich (zejména cenové) dostupnosti. Je tedy zcela zřejmé, že řada právních odvětví se nutně musí potýkat s otázkou, zda vybrané právní předpisy stále více nezaostávají za reálným ekonomickým životem a praktickými potřebami ekonomických subjektů.²⁷

Pokrok v komunikačních a informačních technologiích jednoznačně představuje nová rizika pro ochranu lidských práv a svobod, včetně práv zaměstnanců a zaměstnavatelů. Nové technologie například stírají hranice mezi pracovním a soukromým životem tím, že vytvářejí nové možnosti nárůstu přesčasové práce, možnosti pracovat doma či na zavolání apod. Nové technologie také umožňují zaměstnavatelům mít zaměstnance neustále pod dohledem, „svádějí“ je ke kontrole

²⁵ Zpracování osobních údajů zaměstnavatelů ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů, dostupné na https://www.uoou.cz/vismo/zobraz_dok.asp

²⁶ BARTIK, V., JANEČKOVA, E. Ochrana osobních údajů v aplikační praxi, 4. vydání...

²⁷ MATEJKA, J. Ochrana soukromí na pracovišti dle zákona č. 262/2006 Sb., (nového zákoníku práce). <http://www.itpravo.cz/>.

elektronické pošty, obsahu hlasových komunikací, k monitorování využívání počítačů apod.²⁸

Jde o značně citlivou problematiku, jež má i (resp. především) ústavní aspekty, střetávají se zde zájmy zaměstnanců jako fyzických osob majících ústavně zaručená osobnostní práva (na soukromí, ochranu cti, projevů osobní odvahy apod.) se zájmy zaměstnavatele, jehož cílem je především to, aby jeho zaměstnanci pracovali efektivně a aby byl chráněn jeho majetek. Jelikož jsou osobnostní práva z těch, jejichž účinná ochrana je v každém právním státě esenciální pro to, aby se jako „právní“ vůbec mohl nazývat, a jelikož se uznává, že tato práva jsou nejdůležitější, nejsilnější ze všech (dle literatury „společensky významnější, kvalitně a funkčně vyšší“), a proto mají při střetu s právy jinými zpravidla přednost, musí být postup zaměstnavatele při zajišťování svých zájmů obezřetný a musí vědomě zohledňovat některé relevantní předpisy.²⁹

Předchozí právní úprava (účinná až do konce roku 2006) byla problematická hned v několika ohledech. Klíčovým problémem byla zejména skutečnost, že tehdejší pracovněprávní předpisy ochranu soukromí (respektive přesněji ochranu osobních práv zaměstnanců) neřešily buď vůbec, anebo pouze okrajově. Tehdy platný zákoník práce (zákon č. 65/1965 Sb.) se totiž práv na ochranu soukromí dotýkal pouze výjimečně (šlo zejména o ustanovení § 7 odst. 2, jež poskytuje ochranu před ponižováním lidské důstojnosti účastníka pracovněprávního vztahu, dále pak § 22 odst. 2). Poněkud krkolomně a obtížně se tedy dovozovalo, že v těch případech, které nebyly ošetřeny výslovnou právní úpravou zákoníku práce ani speciálních předpisů, bylo nutné využití analogie iuris, a tedy aplikace ustanovení § 11 a násl. zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů, které se týkaly ochrany osobnosti, a to za podmínky, že to vyžadovala integrita obecných zásad právních a pracovněprávních. Takové řešení se však stále více ukazovalo jako poměrně komplikované, navíc v praxi zřídka kdy docházelo k jeho uplatnění. Právě z těchto důvodů již současný zákoník práce (zákon č. 262/2006 Sb.) na výslovnou úpravu pamatuje. Vzhledem k výše uvedenému, jakož i k tomu, že absence řešení ochrany osobních práv zaměstnance v pracovněprávních vztazích musela „dohánět“ výkladem za použití obecných ústavních východisek vyplývajících z Listiny základních práv a svobod, judikatury Evropského soudu pro lidská práva a za použití § 7 odst. 2 tehdy platného zákoníku práce o postupu

²⁸Hloušková, P., Hofmanová, E., Knebl P., Roučková, D., Schmied, Z., Schweiner, P., Tomandlová, L., *Zákoník práce prováděcí nařízení vláda a další související předpisy k 1. 2. 2018.*, Praha: ANAG, 2018.

²⁹Hansel, M. Problém kamerových systémů instalovaných zaměstnavatelem. *Právo a podnikání* 9/2003, s. 6 a násl.

podle zásad dobrých mravů, objevila se v novém zákoníku tato úprava výslovně. V současné době je ochrana soukromí, resp. právo na soukromí v rámci pracovněprávních vztahů, zakotveno ve čtyřech odstavcích § 316 zákoníku práce, a to v rámci rubriky ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance. Již v názvu této rubriky vyplývá, že prioritou je zde zejména ochrana majetkových vztahů, čemuž pak odpovídá i formulace těchto ustanovení.

Podle tohoto ustanovení (§ 316 odst. 1 zákoníku práce) nesmějí zaměstnanci bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení, přičemž dodržování tohoto ustanovení je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat. Toto ustanovení tak odstraňuje dosavadní stav, kdy nebylo výslovně toto právo nikde zakotveno (snad s výjimkou kontroly práce jako takové). Zákoník práce však dále stanoví určité mantinely této přiměřené kontroly, a to zejména ve vztahu ke kolizi s ochranou soukromí. Zaměstnavatel dále nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci (§ 316 odst. 2). Jak vyplývá z citovaného ustanovení, zákoník práce nepovažuje soukromí na pracovišti za zcela nedotknutelné, ale naopak připouští některé výjimky, a to pro případy závažného důvodu spočívajících ve zvláštní povaze činnosti zaměstnavatele. Zákonodárce zde měl patrně na mysli takové činnosti zaměstnavatele, kde je třeba dbát zvýšených nároků na chování zaměstnanců (např. vzhledem k ochraně utajovaných skutečností, povinnosti mlčenlivosti, ochraně obchodního tajemství apod.). Zákoník práce dále stanoví i určité pojistky proti zneužívání těchto výjimek v těch případech, kdy je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení těchto kontrolních mechanismů (podle § 316 odst. 2). Zaměstnavatel je v těchto případech totiž povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění (§ 316 odst. 3). Znamená to tedy, že má-li zaměstnavatel důvod předpokládaný zákonem, má právo zavést určité kontrolní mechanismy. Zatím nelze říct, o jaké typy zaměstnavatelů (firem) se bude jednat, neboť žádný zákon a zatím ani judikatura blíže nespecifikují, co se rozumí onou zvláštní povahou činnosti.

Současná právní úprava tak doplňuje zásady a principy obsažené v Listině základních práv a svobod a řady dalších mezinárodních dokumentů (např. Úmluva o ochraně lidských práv a základních svobod apod.), přičemž je bezesporu motivována snahou o respektování jak dosavadní právní doktríny, tak i judikatury Evropského soudu pro lidská práva, jehož rozhodovací činnost je v tomto ohledu poměrně pestrá, navíc značně přesahuje existující praxi českých soudů.³⁰ V praxi se často objevují dotazy, zda je možné, aby zaměstnanec v pracovní smlouvě nebo jiné dohodě se zaměstnavatelem vyslovil souhlas s tím, že zaměstnavatel může zaměstnance monitorovat. Takový souhlas nemůže zaměstnanec vyslovit hned z několika důvodů. Základní lidská práva a svobody jsou nezadatelné a nezcizitelné, nepromlčitelné a nezrušitelné. Znamená to, že nikdo jich nemůže být zbaven ani zákonem, ani se jich nemůže zbavit sám tím, že by se jich vzdal ani jako jednotlivec, ani jako příslušník kolektivu. Vedle této ústavní zásady platí § 19 písm. f) zákoníku práce, podle něhož soud přihlédně i bez návrhu k neplatnosti právního úkonu, kterým se zaměstnanec předem vzdává svých práv. Zaměstnanec by se svým souhlasem v pracovní smlouvě předem vzdával svého práva na ochranu soukromí na pracovišti. I kdyby se zaměstnanec vzdal svého práva, nemůže zaměstnavatel zavádět pro kontrolní účely žádná opatření. Výjimka by byla možná v případě závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele.³¹

Opomenout nelze ani judikaturu, a to především judikaturu Evropského soudu pro lidská práva. Zásadním je rozsudek ve věci *Niemietz versus Německo*, kde se soud zabýval výkladem Úmluvy o lidských právech a svobodách, a to konkrétně čl. 8, který stanoví, že „každý má právo na respektování svého soukromého života, obydlí a korespondence, přičemž státní orgán nemůže do výkonu tohoto práva zasahovat, kromě zákonem stanovených případů, a i to pouze v nezbytném rozsahu a okruhu případů“ (např. zájem národní či veřejné bezpečnosti apod.). Evropský soud pro lidská práva v této věci dovedl, že respektování soukromého života musí zahrnovat právo na vytváření a rozvíjení vztahu s dalšími lidskými bytostmi. Dále pak soud rovněž uvedl, že neexistuje důvod pro to, aby způsob chápání pojmu „soukromý život“ vylučoval aktivitu profesní nebo obchodní povahy, protože právě během své pracovní činnosti má většina lidí značnou, ne-li největší příležitost rozvíjet vztahy s vnějším světem.

³⁰ MATEJKA, J. Ochrana soukromí na pracovišti dle zákona č. 262/2006 Sb., (nového zákoníku práce). <http://www.itpravo.cz/>.

³¹ Hloušková, P., Hofmanová, E., Knebl P., Roučková, D., Schmied, Z., Schweiner, P., Tomandlová, L., *Zákoník práce prováděcí nařízení vláda a další související předpisy k 1. 2. 2018.*, Praha: ANAG, 2018.

Obdobná precedentní rozhodnutí však učinil Evropský soud v řadě dalších věcí, přičemž je zřejmé, že ochranu osobních práv zaměstnance na pracovišti je třeba vnímat v širším kontextu než jen v rámci nově zakotvené úpravy, která však bezesporu může sloužit jako dobré vodítko při aplikaci osobních práv člověka nejen na pracovišti, ale i v běžném životě.³²

4.3.1 Kamery na pracovišti

Pohyb na mnoha veřejných prostranstvích nepřetržitě sledují stovky kamer policie, obcí i soukromých firem. V Česku neustále přibývá počet kamerových systémů, které dění na ulicích zaznamenávají. Kamera je jednoznačně nástrojem, který sleduje naše chování v reálném čase, a většina lidí má přirozené obavy, jistou nedůvěru a pocit umenšení osobních svobod. Na druhé straně je nutné zdůraznit, že kamerové systémy slouží k boji s narůstající kriminalitou, k odhalování trestné činnosti, k její prevenci a napomáhají zajistit bezpečnost osob i majetku. Instalace kamerových systémů je účinným pomocníkem při ochraně veřejného pořádku. Kamerové systémy umístěné na úřadech mohou podle zkušeností přispět ke zklidnění mnohdy vypjaté atmosféry mezi klienty a zaměstnanci úřadu a v případě nepříznivého vyústění konfliktní situace má tak úřad k dispozici objektivní záznam.

Kamerové systémy začali také užívat mnozí zaměstnavatelé k monitorování svých zaměstnanců v zaměstnání. Hodlá-li zaměstnavatel na svých pracovištích zřídit kamerový systém, většinou předpokládá, že tento systém může být využit ke dvěma účelům:

- ke sledování, zda zaměstnanci plní své pracovní povinnosti a důsledně využívají pracovní doby
- k ochraně majetku (sledování návštěv, zejména za účelem předcházení krádežím)

Jak už bylo výše uvedeno, zákoník práce však stanoví, že zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze jeho činnosti narušovat soukromí zaměstnance na pracovištích a ve společných prostorách tím, že jej podrobuje otevřenému nebo skrytému sledování. A kamerový systém se záznamem je bezpochyby

³² MATEJKA, J. *Ochrana soukromí na pracovišti dle zákona č. 262/2006 Sb. (nového zákoníku práce)*. <http://www.itpravo.cz/>.

prostředkem sloužícím k otevřenému sledování. Jak už bylo řečeno, v tomto případě nepřichází v úvahu ani možnost instalovat kamerové systémy se souhlasem zaměstnanců, neboť zaměstnanec by se předem vzdával svého práva na ochranu soukromí na pracovišti. Zároveň k vyloučení aplikace tohoto ustanovení nelze použít ani případný souhlas všech zaměstnanců, neboť jak vyplývá z § 4b) odst. 1 zákoníku práce, práva nebo povinnosti v pracovněprávních vztazích mohou být upravena odchýlně od tohoto zákona, jestliže to tento zákon výslovně nezakazuje nebo z povahy jeho ustanovení nevyplývá, že se od něj není možné odchýlit. Od ustanovení uvedených v § 363 je možné se odchýlit jen ve prospěch zaměstnance. V případě § 316 odst. 2 zákoníku práce se však jedná o kogentní ustanovení, které obsahuje pro zaměstnavatele jednoznačný zákaz.

Jedinou možností, jak v souladu se zákonem instalovat kamerové systémy se záznamem, je využití výjimky podle § 316 odst. 3 zákoníku práce, tedy výjimky spočívající ve zvláštní povaze činnosti zaměstnavatele. V jiném případě by se jednalo nejen o porušení zákoníku práce, ale také zákona na ochranu osobních údajů, konkrétně § 10 zákona o ochraně osobních údajů, neboť by zaměstnavatel nedbal na ochranu před neoprávněným zasahováním do soukromého a osobního života zaměstnanců – subjekt údajů.

Jestliže zaměstnavatel dojde k závěru, že se na něj vztahuje výše citovaná výjimka zákoníku práce a instaluje kamerové systémy se záznamem, musí si uvědomit, že tím vstupuje do sféry působnosti zákona o ochraně osobních údajů. Provozování kamerového systému je totiž považováno za zpracování osobních údajů, pokud je vedle kamerového sledování prováděn záznam pořizovaných záběrů a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Jinak řečeno, jedná se o automaticky provozovaný stálý technický systém umožňující pořizovat a uchovávat zvukové, obrazové nebo jiné záznamy ze sledovaných míst, a to např. formou pasivního monitorování prostoru nebo pořizování cílených záběrů (zachycování pohybu) anebo reportážním způsobem.³³

Podle ustanovení § 4 písm. a) zákona o ochraně osobních údajů je osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Údaje

³³*Ochrana osobních údajů na pracovišti*, [online]. Praha, UOOU, 2014. Dostupné z WWW: <http://uoou.cz/assets/File.ashx?id_org=200144id_dokumenty=12691>.

uchovávané v záznamovém zařízení, ať obrazové, či zvukové, jsou tedy osobními údaji pouze za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu (tedy: informace z obrazových či zvukových nahrávek umožňují, byť nepřímo, identifikaci osoby). Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným, jednáním.³⁴

Je třeba konstatovat, že pokud ze zvláštních okolností při pořízení záznamu nebude možné jednotlivé osoby identifikovat, lze v obecné rovině uvést, že informace obsažené v záznamech z kamerových systémů nedosahují kvality osobního údaje, neboť z pouhého záznamu fyzické osoby nelze tuto osobu bez použití dalších doprovodných údajů, v záznamu neobsažených, obecně ztotožnit. Disponuje-li totiž správce osobních údajů snímkem uvedených kvalit, lze jen těžko vyloučit, že by nemohlo k identifikaci příslušné osoby kdykoli v budoucnu dojít, a takováto identifikace je nadto zcela evidentně hlavním důvodem toho, proč k pořizování záznamu vůbec dochází. Lze tedy vyslovit i jistou presumpci dalšího využívání těchto záběrů. Je nepochybné, že pokud by tyto záběry neměly být nijak využívány, celé záznamové zařízení by postrádalo jakýkoli smysl.³⁵ To potvrzuje i stanovisko WP 29³⁶ č. 4/2007 k pojmu osobní údaje přijaté dne 20. června 2007, podle něhož správci údajů často tvrdí, že k identifikaci dojde jen u malé části shromážděného materiálu, a že tedy žádné osobní údaje nejsou zpracovávány, dokud identifikace v těchto několika málo případech skutečně neproběhne. Účelem dohledu pomocí videokamer však je právě identifikace osob zachycených na záznamu ve všech případech, kdy to správce pokládá za nezbytné. Celý systém jako takový se proto musí považovat za zpracovávání údajů o identifikovatelných osobách, i když některé osoby zachycené na záznamu v praxi identifikovatelné nejsou.

³⁴Stanovisko č. 1/2006, [online]. Praha, UOOU, 2006. Dostupné z WWW: <http://uouu.cz/vismo/dokumenty2.asp?id_org=200144id=stanovisko/provozovani_kameroveho_systemu=1099>.

³⁵Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Praha, UOOU, 2006. Dostupné z WWW: <http://uouu.cz/vismo/dokumenty2.asp?id_org=200144id=stanovisko/provozovani_kameroveho_systemu=1099>.

³⁶ Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jde o nezávislý evropský poradní orgán pro ochranu údajů a soukromí. Jeho úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Z toho vyplývá, že zaměstnavatel se instalací kamerového systému se záznamem stává správcem osobních údajů ve smyslu § 4 písm. j) zákona o ochraně osobních údajů, a vztahují se na něj všechny povinnosti tak, jak byly popsány v kapitole II. Některé problémy při zpracování osobních údajů v souvislosti se správou nemovitostí.

Ani využití výjimky podle § 316 odst. Zákoníku práce tedy neznamená, že by zaměstnavatel mohl monitorovat zaměstnance bez omezení. Jak již bylo několikrát řečeno, i na pracovišti by měl zaměstnanec mít jistou minimální úroveň soukromí zaručenu. To se může týkat např. nezbytných soukromých telefonických hovorů, (rovněž nezbytné) elektronické korespondence, činnosti v průběhu přestávek v práci, osobních věcí, které má zaměstnanec na pracovišti apod. Je nutné si uvědomit, že striktní kontrola v podobě, v jaké byla shora nastíněna, nemusí nutně vést k zefektivnění práce. Pracuje-li člověk pod tlakem a s vědomím, že je zcela pod kontrolou, rozhodně jej to nebude ovlivňovat příznivě. Existuje názor (kladoucí na jednotlivce etický a svým způsobem i estetický nárok), že člověk by se v soukromí měl chovat vždy jen tak, jak by se choval ve společnosti. To není možné. Člověk se v soukromí bude chovat vždy jinak, uvolněněji než na veřejnosti (ať si to přizná, nebo ne), a ani jinak nemůže. Rovněž se bude chovat jinak na pracovišti, o kterém ví, že je pod stálým dohledem, než na pracovišti, které pod takovým dohledem není. Jistě, docílí se toho, že nebude na internetu hledat vtipy, ale docílí se toho, že bude např. pracovat ve stresu, v domnění, že každé přirozené uvolnění či odpočinek někdo může vidět a že mu to bude vyčteno či že za to bude postižen.³⁷

4.3.2 Monitorování služebních telefonů

Další oblastí, kde se velmi často objevuje snaha zaměstnavatel monitorovat počínání svých zaměstnanců, je používání služebních telefonů. Jedná se o pevné linky i o mobilní telefony. A právě především u mobilních telefonů ve většině případů existují pravidla pro jejich využívání ať již služebně, nebo soukromě. Telefony obvykle mohou zaměstnanci používat také k soukromým hovorům. Typickým způsobem řešení, jak odlišit soukromé a služební hovory, bývá povinnost soukromý hovor označit nějakým předem stanoveným způsobem, např. předvolbou (symbol) před vytáčeným telefonním číslem.

³⁷ HANSEL, M. Problém kamerových systémů instalovaných zaměstnavatelem. *Právo a podnikání* 9/2003, s. 6 a násl.

Obecně je možné říct, že není málo případů, kdy si zaměstnavatelé pořizují různá technická zařízení, která umožňují zjistit telefonní čísla, na která zaměstnanec telefonuje. To platí především u pevných linek. Zaměstnavatel je přitom veden dobrou snahou, aby zaměstnanec vyřizováním soukromých záležitostí nezvyšoval náklady zaměstnavatele za telefonní služby a plně se věnoval zaměstnání. I při řešení těchto problémů je nutno postupovat podle ústavních zásad a předpisů, které je rozpracovávají. Tajemství obsahu telefonních zpráv podléhá ochraně podle trestního zákona a je zaručeno Listinou základních práv a svobod. Znamená to, že nikdo, tedy ani zaměstnavatel, nemůže odposlouchávat hovory zaměstnance, i když by se jednalo o soukromé rozhovory nebo zařizování soukromých záležitostí pomocí telefonu na pracovišti a v pracovní době.

Nelze však zapomínat, že za určitých okolností může být a pravděpodobně také bude aplikovatelný zákon o ochraně osobních údajů. Bude-li zaměstnavatel systematicky shromažďovat údaje o zaměstnanci, o tom, kolik soukromých hovorů za měsíc učinil ze služebního telefonu, a především na jaká telefonní čísla, bude se nepochybně jednat o zpracování osobních údajů ve smyslu § 4 písm. e) zákona o ochraně osobních údajů. To, že zaměstnavatel tyto údaje shromažďovat a zpracovávat bude, je zcela nepochybné, neboť musí tyto informace vést a faktury za telefonní hovory archivovat pro účely účetnictví. Vzhledem k tomu, že se tedy jedná o zpracování osobních údajů, musí zaměstnavatel i při zpracování těchto údajů splnit všechny povinnosti vyplývající ze zákona o ochraně osobních údajů. Beze sporu se bude jednat o zpracování bez souhlasu v rámci výjimky § 5 odst. 2 písm. a) zákona o ochraně osobních údajů, podle něhož může správce zpracovávat osobní údaje bez souhlasu subjektu údajů, jestliže provádí zpracování nezbytné pro dodržování právní povinnosti. Chce-li tedy zaměstnanec, aby jeho soukromé hovory zůstaly skutečně soukromé, tedy aby nebylo zřejmé, na jaká telefonní čísla bylo voláno a jak často, měl by zvážit, zda je vhodné k takovým hovorům použít služební telefon.³⁸

4.3.3 Monitorování služebních automobilů

Vzhledem k tomu, že náklady na provoz služebních vozidel jsou nepoměrně vyšší než na užívání služebních telefonů, objevila se samozřejmě určitá snaha o

³⁸ BARTIK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*. Praha 2016. s. 131

monitoring i u nich. Je obtížné přesně spočítat, kolik prostředků skutečně stojí provoz firemních automobilů. Jednoduché není například rozlišit soukromou cestu od služební nebo poznat, kde a kdy se automobil pohyboval. Každý podnikatel má nepochybně právo mít přesnou kontrolu nad vynaloženými finančními prostředky a jejich optimálním využíváním.

Moderní technika však v mnohém situaci usnadňuje. Monitorovací systém obvykle využívá přijímač signálu GPS, který určuje přesnou polohu vozidla v libovolně zvoleném časovém nebo délkovém intervalu a získanou informaci ukládá do své paměti. Tyto údaje lze pak jednoduchým způsobem přehrát do počítače, kde je speciální počítačový software porovná s příslušnou digitální mapou a vyhotoví podrobný itinerář jízd. Součástí je také vyhodnocení spotřeby pohonných hmot nebo měsíční a roční zúčtování.

Objevily se případy, kdy se zaměstnavatel pokusil vybavit všechna svá vozidla satelitním vyhledávacím a monitorovacím zařízením (zejména pro prevenci krádeží a monitoringu využití vozidel v pracovní době jejich řidičů), aniž by na to upozornil své zaměstnance. Bez ohledu na to, že se zjistilo, že řada zaměstnanců zneužívá služební automobily v největší možné míře a že někteří se snažili oklamat systém, objevila se ze strany některých zaměstnanců námitka, že v případě použití tohoto systému v době oprávněného užívání vozidla k soukromým účelům se bude jednat o zásah do práv dotčených zaměstnanců, bude-li mít zaměstnavatel informace o jejich pohybu.

Jak už bylo uvedeno výše, zákon o ochraně osobních údajů se vztahuje na zpracování osobních údajů, kterým je v § 4 písm. e) tohoto zákona definovaná operace nebo soustava operací prováděná s osobními údaji systematicky. Na namátkové kontroly, tedy na nesystematické zpracování se zákon o ochraně osobních údajů vztahovat nebude.

Při posouzení toho, zda ke zpracování osobních údajů dochází, je vždy nutné vycházet ze stanoveného účelu. V uvedeném případě by se o zpracování osobních údajů jednalo, jestliže by účelem instalace satelitního sledovacího zařízení bylo systematické shromažďování údajů o všech zaměstnancích, kteří firemní auto používají, a další zpracování těchto údajů. Z toho vyplývá, že zákon o ochraně osobních údajů se při dodržení výše uvedených pravidel nevztahuje ani na monitorování oprávněného užívání vozidla k soukromým účelům, ovšem bez ohledu na to by bylo v souladu s dobrými

mrawy získat souhlas zaměstnanců k monitorování automobilu i při oprávněném užívání vozidla k soukromým účelům.

4.3.4 Monitorování e-mailové pošty zaměstnanců

Rozvíjející se výpočetní technika a snaha o zvýšení efektivity práce umožňuje zaměstnavatelům zavádět elektronickou poštu na většinu pracovišť. Vedle kladů, které tato technika přináší, se objevují praktické problémy. Např. zda zaměstnavatel může kontrolovat elektronickou poštu, kterou zaměstnanec obdržel na pracoviště do schránky počítače, který mu byl svěřen k výkonu práce, nebo poštu, kterou zaměstnanec obdržel. Při právním posuzování takového případu musíme vycházet z Listiny základních práv a svobod (čl. 13), která zaručuje ochranu listovního tajemství, a ze zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník“) - § 182. Listina základních práv a svobod stanoví, že nikdo nesmí porušit listovní tajemství jiných písemností a záznamů ať již uchovávaných v soukromí, nebo zasílaných poštou, anebo jiným způsobem. Výjimkou jsou případy, které jsou uvedeny ve zvláštním právním předpisu (např. vyšetřování trestného činu). Ústavní zásadu ochrany listovního tajemství rozpracovává trestní zákoník. Trestného činu podle § 182 (porušení dopravovaných zpráv) se dopustí ten, kdo úmyslně poruší tajemství uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením, datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data, bude potrestán odnětím svobody na dvě léta nebo zákazem činnosti.

Pokud jde o monitorování elektronické pošty zaměstnanců ze strany jejich zaměstnavatelů, je nutno mít na zřeteli, že i elektronická pošta je poštou, a i písemnosti v elektronické podobě jsou písemnosti, a i pro ně platí obdobná pravidla jako pro ostatní písemnosti. Při posuzování otázky monitorování elektronické pošty je tedy nutno vzít v úvahu především článek 13 Listiny základních práv a svobod. Na něj navazuje ustanovení § 81 občanského zákoníku, které mimo jiné stanoví, že ochrany požívají

zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy. Dále je z těchto ustanovení zřejmé, že dopadají na každého, a tedy i na zaměstnavatele a zaměstnavatel tato ustanovení musí respektovat. V diskuzi o tom, zda soukromá zpráva doručená zaměstnanci pomocí elektronických komunikačních sítí je i po doručení zprávou soukromou, či nikoliv, je nutno vzít v úvahu Směrnici Evropského parlamentu a Rady z roku 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), kterou musela Česká republika promítnout do svého právního řádu před vstupem do EU. Ve smyslu této Směrnice je uživatelem jakákoli fyzická osoba používající veřejnou elektronickou komunikační službu pro soukromé či obchodní účely, přičemž není nezbytně nutné, aby byla účastníkem této služby.

Na druhé straně je však nutno vnímat i to, že zaměstnavatel má právo sledovat u svých zaměstnanců dodržování pracovní doby a jejího využití. Pro výkon tohoto práva nemá zaměstnavatel právo sledovat, monitorovat a zpracovávat obsah korespondence svých zaměstnanců. Zaměstnavatel by případně mohl pouze sledovat počet e-mailů došlých a odeslaných u svých zaměstnanců a požadovat, aby své soukromé záležitosti v pracovní době a na pracovišti vyřizovali v přiměřené a více méně v nezbytné míře, neboť jak bylo výše uvedeno, ani pracovněprávní vztah neodstraňuje právo na přiměřené soukromí zaměstnanců. O svém záměru či praxi sledovat četnost přijímaných či odesílaných e-mailových zpráv by měl zaměstnavatel předem své zaměstnance uvědomit, a to nejlépe při navazování pracovního vztahu. K uvedenému účelu by měla existovat obecná pravidla pro zaměstnavatele a zaměstnance, z nichž by mělo být jasné, že obsah pošty je chráněn a že ve vztahu k němu se ctí listovní tajemství i ochrana osobních údajů.

Z pohledu ochrany osobních údajů je však nutné mít na zřeteli ještě další otázku, a sice zda vždy při monitorování e-mailové pošty dochází ke zpracování osobních údajů. K tomu by docházelo tehdy, pokud by zaměstnavatel svou činností systematicky monitoroval své zaměstnance a údaje získané z této činnosti by dále zpracovával. V takovém případě by na tuto činnost zaměstnavatele dopadal v plném rozsahu zákon o ochraně osobních údajů. Pokud by však zaměstnavatel e-mailovou poštu nesledoval systematicky, ale jen nahodile by ji prohlédl (např. z důvodu, že jeho zaměstnanec je dlouhodoběji nepřítomen na pracovišti), a to pro to, že je třeba vyřídit pracovní korespondenci, pak by se zřejmě nejednalo o zpracování osobních údajů, a zákon o

ochraně osobních údajů by tedy na tento postup nedopadal. K danému problému je vhodné uvést, že zaměstnavatel v žádném případě nemůže sledovat obsah korespondence, a tedy ani korespondence v elektronické podobě svých zaměstnanců, případně dalších osob. K otázce monitoringu elektronické pošty se vyjádřil také Úřad ve svém Stanovisku č. 2/2009³⁹ „Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště“, když uvádí, že „elektronické dokumenty jsou písemnostmi, byť nejsou listinami. Proto pro ně platí stejná pravidla jako pro ostatní písemnosti.

4.4 Fotografie v osobním spisu zaměstnance z hlediska zákona o ochraně osobních údajů

Jednou ze součástí osobního spisu bývá fotografie zaměstnance. Důvodů, pro něž zaměstnavatelé fotografie vyžadují, je mnoho. Nejčastěji bývají uváděny důvody bezpečnostní (především u velkých zaměstnavatelů, kde se jednotliví zaměstnanci navzájem neznají), druhým nejčastějším důvodem je umístění na intranetu (účel je v zásadě stejný jako u bezpečnostních důvodů). Pokud zaměstnavatel hodlá fotografii zaměstnance využít, musí vzít v potaz i zákon o ochraně osobních údajů.

Podle ustanovení § 4 písm. a) zákona o ochraně osobních údajů je osobním údajem jakákoliv informace týkající se určeného nebo určitého subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. Z pořízené fotografie lze ve většině případů subjekt údajů identifikovat, samozřejmě v závislosti na kvalitě této fotografie. Jsou-li proto portrétní fotografie systematicky zpracovávány, jedná se nepochybně o zpracování osobních údajů ve smyslu zákona o ochraně osobních údajů. Častým dotazem bývá, zda se při uchovávání fotografií nejedná také o zpracování citlivých osobních údajů. Uchovávání fotografií není samo o sobě posuzováno jako zpracování citlivých údajů vypovídajících o rasovém nebo etnickém původu, pokud nedochází k dalšímu zpracování, například třídění subjektu údajů podle biometrických charakteristik vypovídajících na fotografii o

³⁹ Dostupné na http://www.uouu.cz/files/stanovisko_2009_2.pdf.

rasovém nebo etnickém původu, připojování slovně vyjádřených údajů o rasovém nebo etnickém původu k jednotlivým fotografiím a podobně.

Běžné uchovávání portrétních fotografií v datovém souboru je proto možné podřídit ustanovení § 5 odst. 2 zákona o ochraně osobních údajů. Portrétní fotografie bývají nejčastěji uchovávány zaměstnavatelem, a to za různými účely. Jsou-li tyto fotografie uchovávány a dále zpracovávány pouze za účelem vydání služebního průkazu, bude se z hlediska zákona o ochraně osobních údajů jednat o zpracování ve smyslu § 5 odst. 2 písm. a), tedy zpracování nezbytné pro dodržení právní povinnosti správce, tedy zaměstnavatele. Pro takové zpracování se pak nevyžaduje souhlas zaměstnance, dá se říci, že naopak, bude-li jeho pracovní náplní činnost, pro kterou na základě právních předpisů je třeba služebního průkazu vydávaného zaměstnavatelem, je jeho povinností fotografii zaměstnavateli poskytnout. Ten pak vázán právním předpisem ji může použít právě jen pro stanovený účel. Při zpracování za jiným účelem je třeba posuzovat, zda je pro zpracování fotografií bez souhlasu subjektu údajů splněna například výjimka podle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, tedy je-li to nezbytné pro ochranu práv a právem chráněných zájmů správce. Je dále otázkou, jaký je účel uchovávání fotografií zaměstnanců v databázovém systému zaměstnavatele a zda je tento účel nezbytný pro ochranu práv zaměstnavatele, to závisí na charakteru činnosti zaměstnavatele.

Nejsou-li však shromažďovány portrétní fotografie, tedy podobizny jednotlivých subjektů údajů, ale pouze fotografie zachycující průběh různých akcí a tyto fotografie jsou označeny jen názvem akce nikoli údaji, z nichž by bylo možné identifikovat subjekty údajů, nejedná se o zpracování osobních údajů ve smyslu § 4 písm. e) zákona o ochraně osobních údajů a při jejich zpracování tak nedochází k zásahu do práva na ochranu osobních údajů.⁴⁰

Jak bylo uvedeno výše, jsou-li fotografie zaměstnanců zpracovávány pouze za účelem vydání služebního průkazu, bude se z hlediska zákona o ochraně osobních údajů jednat o zpracování ve smyslu § 5 odst. 2 písm. a), tedy zpracování nezbytné pro dodržení právních povinností správce, tedy zaměstnavatele. V takovém případě je nutné posoudit existenci zákona, který by stanovil tuto povinnost. Obecný právní předpis, tedy zákoník práce, žádnou takovou povinnost zaměstnavateli neukládá, stejně tak ani

⁴⁰ BARTIK, V., JANEČKOVÁ, E. Ochrana osobních údajů v aplikační praxi. 2. vydání. Praha: Linde, str. 153 a násl.

například zákon č. 312/2002 Sb., o úředních územních samosprávních celcích a o změně některých zákonů, ve znění pozdějších předpisů. Naopak zákon č. 234/2014 Sb., o státní službě, v ustanovení § 154 (služební průkaz) stanoví, že Služební úřad, v němž státní zaměstnanec vykonává službu, vystaví státnímu zaměstnanci služební průkaz. Služební průkaz osvědčuje, že jeho držitel je státním zaměstnancem. Služební průkaz obsahuje a) fotografii státního zaměstnance, b) jméno, popřípadě jména a příjmení, popřípadě i akademický titul státního zaměstnance, c) evidenční číslo státního zaměstnance, d) označení služebního úřadu, v němž státní zaměstnanec vykonává službu, e) číslo služebního průkazu a f) datum vystavení, popřípadě i datum platnosti služebního průkazu. Tento předpis tak přímo ukládá služebnímu orgánu, který plní funkci zaměstnavatele, zpracování fotografie a také stanoví, pro jaký účel má být použita. Přímé zákonné zmocnění ke zpracování fotografie zaměstnance lze nalézt jen velmi sporadicky. Příkladem může být zákon č. 266/1994 Sb., o drahách, který v § 58 odst. 5 stanoví, že pověření k výkonu státního dozoru nebo vrchního státního dozoru ve věcech drah ve formě průkazu vydává správní orgán, do jehož působnosti výkon dozoru spadá. Náležitosti průkazu a jeho vzor stanoví prováděcí právní předpis. Tímto předpisem je pak vyhláška č. 9/2015 Sb., o stanovení náležitostí a vzorů pověření k výkonu státního dozoru, státního odborného dozoru, vrchního státního dozoru a vrchního státního odborného dozoru v dopravě ve formě průkazu a o změně souvisejících vyhlášek. Ta pak v ustanovení § 1 odst. 1 stanoví, že pověření k výkonu státního dozoru a vrchního státního dozoru ve věcech pozemních komunikací ve formě průkazu obsahuje mimo jiné i fotografii pověřené osoby o rozměrech 35 x 45 mm, jejíž spodní okraj je přelepen holografickou přelepku s textem „ČESKÁ REPUBLIKA“.

Stejně tak zákon č. 187/2006 Sb., o nemocenském pojištění, v ustanovení § 76 odst. 3 ukládá, že pověření zaměstnanci orgánu nemocenského pojištění provádějící kontrolu dodržování režimu dočasně práce neschopného pojištěnce jsou povinni se prokázat průkazem s fotografií vydaným orgánem nemocenského pojištění. Je však mnoho předpisů podzákonných, vesměs vyhlášek, které upravují a ukládají, zejména v souvislosti s nějakým oprávněním zpracovávat i fotografie osob, kterým se vydává služební průkaz apod.

Ve všech těchto případech se bude z hlediska zákona o ochraně osobních údajů jednat o zpracovávání ve smyslu § 5 odst. 2 písm. a), tedy zpracování nezbytné pro dodržení právní povinnosti správce – zaměstnavatele. Pro takové zpracování se pak nevyžaduje souhlas zaměstnance, dá se říci, že naopak, bude-li jeho pracovní náplní

činnost, pro kterou na základě právních předpisů je třeba služebního průkazu vydaného zaměstnavatelem, je jeho povinností fotografii zaměstnavateli poskytnout. Ten pak, vázán právním předpisem, ji může použít právě jen pro stanovený účel. Jakékoliv jiné využití (zpracování) fotografie je již vázáno na souhlas zaměstnance. Bude tak třeba takového souhlasu například ke zpřístupnění fotografie v interním informačním systému, v elektronickém telefonním seznamu apod.

Nevejde-li se zaměstnavatel do výjimek stanovených v jednotlivých písmenech § 5 odst. 2 zákona o ochraně osobních údajů, a bude-li přesto chtít použít fotografii zaměstnance, bude muset získat jeho souhlas. Zpracování osobních údajů se souhlasem subjektu údajů je jednou ze základních zásad zpracování osobních údajů, a to proto, že zpracováním osobních údajů dochází k zásahu do soukromí jejich nositele. Obecně je poskytnutí souhlasu právním úkonem, respektive právním jednáním, a to právním jednáním, které je svým charakterem jednoznačně jednáním jednostranným. Nejedná se tedy o dohodu mezi správcem nebo zpracovatelem na straně jedné, a subjektem údajů – fyzickou osobou na straně druhé. Pro posouzení jeho platnosti je proto nutné vzít v potaz i úpravu právních jednání v obecném právním předpisu, jímž je v tomto případě občanský zákoník.

Podle definice zákona o ochraně osobních údajů je souhlas svobodným projevem vůle. A právě svoboda souhlasu je většinou tou nejproblematictější vlastností, kterou lze u již udělených souhlasů často zpochybnit. Jak už bylo řečeno výše, souhlas se zpracováním osobních údajů je svým charakterem jednostranným právním jednáním a ani jeho zpracováním do dokumentu, který je součástí dvoustranného právního vztahu, se ze souhlasu nestává úkon dvoustranný. Tento krok může subjekt údajů zmást, případně uvést v omyl. Je tedy otázkou, zda takovýto úkon je úkonem, který splňuje parametry právního jednání podle občanského zákoníku, když onen volní prvek je vzhledem k výše uvedenému zpochybnitelný. Začlenění souhlasu s používáním fotografie do pracovní smlouvy není proto nejvhodnějším řešením.

Souhlasem subjektu údajů je dále vědomý projev vůle, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů. Jak již bylo řečeno, u souhlasu se zpracováním osobních údajů, jež citlivé nejsou, podmínka výslovnosti v zákoně o ochraně osobních údajů není stanovena. Takovýto souhlas může tedy být poskytnut i konkludentně, respektive jinak než výslovně. Subjekt údajů například může po obdržení patřičné informace své osobní údaje správci poskytnout, čímž mlčky, ne výslovně,

souhlasí s jejich zpracováním. K určení obsahu vůle může totiž sloužit i širší kontext jednání, případně i jednání následného, jestliže je z něho možné na obsah vůle zpětně usuzovat. Zákon o ochraně osobních údajů pro souhlas se zpracováním osobních údajů nestanoví povinnou formu, například písemnou. V této souvislosti je rovněž třeba poukázat na § 5 odst. 4 větu druhou zákona o ochraně osobních údajů, která stanoví, že správce musí být po celou dobu zpracování schopen prokázat, že mu subjekt údajů ke zpracování poskytl svůj souhlas. V případě konfliktní situace, kdy subjekt údajů bude tvrdit, že správce zpracovává jeho osobní údaje bez souhlasu, je tady důkazní břemeno na straně správce. V tomto případě bude správce povinen prokázat, že subjekt údajů se zpracováním souhlasil a že souhlas splňoval všechny výše uvedené náležitosti.

Aby bylo možné udělený souhlas skutečně považovat za vědomý, je nutné, aby byl také takzvaně informovaný. Tuto informovanost vyžaduje již zmiňované ustanovení § 5 odst. 4, podle něhož musí být subjekt údajů při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci na jaké období, a dále § 11 odst. 1 a 2 zákona o ochraně osobních údajů, které vyžadují, aby správce při shromažďování osobních údajů subjekt informoval o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21. V případě, kdy správce zpracovává osobní údaje získané od subjektu údajů, musí subjekt údajů poučit o tom, zda je poskytnutí osobního údaje povinné, či dobrovolné. Je-li subjekt údajů povinen podle zvláštního zákona osobní údaje pro zpracování poskytnout, poučí jej správce o této skutečnosti, jakož i o následcích odmítnutí osobních údajů.

Tyto podmínky je ale nutno vykládat pouze v celém kontextu souboru práv a povinností správce podle zákona o ochraně osobních údajů a dbát na to, že přes udělený souhlas je nutno, aby správce dodržoval i další principy ochrany dat, a to především legitimitu, přiměřenost a účelnost zpracovávaných osobních údajů.⁴¹

Jak již bylo uvedeno, v souladu s ustanovením § 5 odst. 4 zákona o ochraně osobních údajů musí subjekt údajů být při udělení souhlasu informován o tom, pro jaký

⁴¹ BARTÍK, V., JANEČKOVÁ, E. Zákon o ochraně osobních údajů s komentářem. Olomouc, 2010, str. 63 a násl.

účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období.

Podmínku prokazatelného souhlasu také může splňovat seznam zaměstnanců s podpisem souhlasu ke zpřístupnění nebo zveřejnění fotografie, a to v případě, že bude zaměstnavatel schopen prokázat, že zaměstnanci poskytli všechny relevantní informace.

V případě, že zaměstnavatel bude využívat fotografii za jiným účelem, než mu stanoví zákon, nesmí zapomenout splnit oznamovací povinnost tak, jak ji stanoví § 16 zákona o ochraně osobních údajů. Podle něj ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle tohoto zákona, s výjimkou zpracování uvedených v § 18, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováním osobních údajů. Tuto povinnost je tedy třeba splnit ještě před tím, než vůbec ke zpracování dojde. Odstavec 2 tohoto ustanovení specifikuje rozsah informací, které musí správce osobních údajů sdělit Úřadu. Jedná se o údaje, které se týkají správce (identifikační údaje správce, u fyzické osoby, která není podnikatelem, jméno, popřípadě jména, příjmení, datum narození a adresu místa trvalého pobytu, u jiných subjektů obchodní firmu nebo název, sídlo a identifikační číslo, pokud bylo přiděleno, a jméno, popřípadě jména, a příjmení osob, které jsou jejich statutárními zástupci), údaje dokládající splnění některých základních povinností (účel nebo účely zpracování, popis způsobu zpracování osobních údajů, popis opatření k zajištění ochrany osobních údajů podle § 13) a údaje, které zpřesňují charakteristiku zamýšleného zpracování (kategorie subjektu údajů a osobních údajů, které se těchto subjektů týkají, zdroje osobních údajů, místo nebo místa zpracování osobních údajů, příjemce nebo kategorie příjemců, předpokládaná předání osobních údajů do jiných států).

Oznámení o zpracování osobních údajů, případně oznámení o změně zpracování osobních údajů, musí obsahovat všechny informace požadované v ustanovení § 16 odst. 2 zákona o ochraně osobních údajů, jinak oznámení o úmyslu správce zpracovávat osobní údaje Úřad nemůže zaregistrovat.

Jak vidno, i tak zdánlivě jednoduchá a samozřejmá věc, jako je obyčejná fotografie, může v některých případech způsobit problémy, respektive je třeba při nakládání s ní respektovat skutečnost, že i využívání fotografie zaměstnanců má svůj právní režim, který je třeba dodržovat. Není ani zdaleka samozřejmostí, aby zaměstnavatel jen tak bez

dalšího disponoval fotografiemi svých zaměstnanců, a dokonce jich využíval k jakýmkoliv účelům.⁴²

4.5 Poskytování osobních údajů o zaměstnancích

S problematikou poskytování informací o zaměstnancích se zaměstnavatelé setkávají poměrně často. Je přitom zřejmé, že zaměstnavatelé disponují relativně velkým rozsahem informací, osobních údajů, které se vztahují k jednotlivým zaměstnancům. Jsou to jednak údaje, které zaměstnavatel potřebuje pro dodržení a plnění svých zákonných povinností, a často také informace, které byly od zaměstnance získány a dále jsou zpracovávány s jeho souhlasem. Zákoník práce, na rozdíl od předchozí právní úpravy, dává v § 312 zaměstnavatelům přímé oprávnění vést osobní spis zaměstnance. Osobní spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v pracovněprávním vztahu, a dále je stanoveno, že do osobního spisu mohou nahlížet vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízení. Právo nahlížet do osobního spisu má orgán inspekce práce, Úřad práce České republiky, Úřad pro ochranu osobních údajů, soud, státní zástupce, policejní orgán, Národní bezpečnostní úřad a zpravodajské služby.

Z pohledu zákona o ochraně osobních údajů je tak zcela v souladu s jeho ustanovením § 5 odst. 1 písm. d) respektována povinnost shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Tímto účelem je plnění zákonných povinností zaměstnavatele stanovených buď přímo zákoníkem práce, nebo jinými právními předpisy. Z práva nahlížet do osobního spisu plyne, že výše uvedené orgány mají právo na informace o zaměstnanci v osobním spisu uvedené. Nikoliv však bezbřezě, ale toliko na ty, které potřebují k plnění svých vlastních povinností. Tato jejich oprávnění jsou pak „zrcadlově“ vyjádřena v dalších zvláštních právních předpisech, jako je např. zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů (dále jen „trestní řád“), a jeho ustanovení § 8⁴³ za podmínek tam stanovených, nebo také § 128 občanského soudního řádu⁴⁴ a mnohé další.

⁴² BARTÍK, V., JANEČKOVÁ, E., Fotografie v osobním spisu zaměstnance z hlediska zákona o ochraně osobních údajů, In PaM 9/2012

⁴³ § 8 Státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhotovovat dožádáním orgánům činným v trestním řízení při plnění

Je však také stanoven okruh osob kromě zaměstnavatele, které se s údaji o zaměstnanci mohou seznámit, a to formou nahlížení do spisu. Jedná se výlučně o vedoucí zaměstnance, kteří jsou konkrétnímu pracovníkovi nadřizení, a tedy nikoli o jakéhokoliv vedoucího zaměstnance. Z logiky věci plyne, že osoby, které mají v pracovní náplni vedení osobních spisů zaměstnanců, mají právo do těchto spisů nahlížet také, neboť je doplňují o nezbytné písemnosti, jež spis obsahovat má. Na druhou stranu platí, že účel vedení osobního spisu je dán a není možné využívat informace z osobních spisů pro jiné účely.

Je tak vyloučeno například zveřejňovat data narození zaměstnanců, byť by to bylo s dobrým úmyslem gratulace k narozeninám, což koneckonců může být i součástí „firemní kultury“. Takové nakládání s osobními údaji je možné jen se souhlasem dotčeného zaměstnance.

S poskytováním osobních údajů zaměstnanců úzce souvisí i povinnost mlčenlivosti. Obecná povinnost mlčenlivosti ve vztahu k osobním údajům zaměstnanců *expressis verbis* v zákoníku práce není. Ten sice obsahuje povinnost mlčenlivosti, ale ta se týká jen omezeného okruhu zaměstnanců. První skupinou zaměstnanců, jimž je povinnost mlčenlivosti uložena, jsou členové odborové organizace, rady zaměstnanců a zástupce pro oblast bezpečnosti a ochrany zdraví a odborníci, které si zástupci zaměstnanců k výkonu svých oprávnění přizvou.⁴⁵

Druhá skupina zaměstnanců, jimž je uložena povinnost mlčenlivosti, je uvedena v § 303 odst. 1 zákoníku práce. Stručně řečeno, jedná se o zaměstnance „veřejné správy“. V širokém slova smyslu. Těm je mimo jiných obecných povinností uložených všem zaměstnancům (například § 106 odst. 4 zákoníku práce) uložena také povinnost mlčenlivosti⁴⁶.

Jak již bylo uvedeno, zákoník práce neukládá ve vztahu k informacím o zaměstnancích, které jsou uvedeny v osobním spise, obecnou povinnost mlčenlivosti

jejich úkolů. Státní orgány jsou dále povinny neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin.

⁴⁴ § 128 Každý je povinen bezplatně na dotaz sdělit soudu skutečnosti, které mají význam pro řízení a rozhodnutí. Ustanovení § 139 odst. 3 tím není dotčeno. Odmítnout soudu sdělit tyto skutečnosti může jen ten, kdo by tak mohl učinit jako svědek podle § 126 odst. 1.

⁴⁵ § 276 odst. 3 a 4

⁴⁶ § 303 odst. 2 psím. B) ...zachovávat mlčenlivost o skutečnostech, o nichž se dozvěděli při výkonu zaměstnání a které v zájmu zaměstnavatele nelze sdělovat jiným osobám, to neplatí, pokud byli této povinnosti zproštěni statutárním orgánem nebo jím pověřeným vedoucím zaměstnancem, nestanoví-li zvláštní předpis jinak.

přímo. Přesto ji obsahuje v tom smyslu, že § 312 odst. 2 stanoví taxativně, kdo do spisu může nahlížet. Z hlediska zaměstnavatele se jedná toliko o vedoucí zaměstnance, a to ještě jen ty, kteří jsou zaměstnanci nadřízeni. Přitom nadřízenost je zjevně míněna v celé hierarchii řídicích pracovníků konkrétního zaměstnance, nikoliv jen jeho přímý nadřízený. Přímá povinnost mlčenlivosti je upravena v § 314 odst. 2 tak, že jiné informace o zaměstnanci než ty, které mohou být obsahem pracovního posudku, je zaměstnavatel oprávněn o zaměstnanci podávat pouze s jeho souhlasem, nestanoví-li zvláštní právní předpis jinak. Povinnost mlčenlivosti je tedy nutné ze zákoníku práce dovozovat v celém rozsahu kontextuálně, nicméně je zjevné, že povinnost mlčenlivosti tu existuje. Současně je však povinnost mlčenlivosti stanovena i v § 15 zákona o ochraně osobních údajů. A protože se v rámci personální práce, a nejen v ní, jedná z hlediska zákona o ochraně osobních údajů o zpracování osobních údajů, zaměstnavatel má postavení správce osobních údajů, bude zmíněný § 15 zákona o ochraně osobních údajů přímo aplikovatelný i na zmíněná zpracování. Citované ustanovení je pojato poměrně široce⁴⁷, a co je však důležité, je fakt, že porušení mlčenlivosti zaměstnance může zaměstnavatel postihnout pouze nástroji, které mu zákoník práce dává, tedy nejčastěji pravděpodobně jako porušení pracovní kázně. Za porušení mlčenlivosti stanovené zákonem o ochraně osobních údajů lze uložit pokutu, neboť skutková podstata přestupku podle § 44 odst. 1 zákona o ochraně osobních údajů je svázána právě s povinností mlčenlivosti. Pokutu lze uložit až do výše 100 000 Kč.

Obecná povinnost mlčenlivosti se však vztahuje i na jiná zpracování osobních údajů, i když se nejedná přímo o zpracování osobních údajů vedených v osobním spise zaměstnance. Zákoník práce stanoví zaměstnavatelům i řadu povinností, které jsou povinni plnit a při kterých dochází ke zpracování osobních údajů.

Zaměstnavatelé jako správci osobních údajů však disponují mnohem větším rozsahem osobních údajů než jen těmi, které jsou shromážděny a zpracovávány v osobním spise zaměstnance. Lze dokonce říci, že zákoník práce předepisuje zaměstnavatelům shromažďovat a dále zpracovávat v některých případech i citlivé

⁴⁷ §15 (1) Zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací. (2) Ustanovení předchozího odstavce není dotčena povinnost zachovávat mlčenlivost podle zvláštních zákonů. (3) Povinnost zachovávat mlčenlivost se nevztahuje na informační povinnost podle zvláštních zákonů.

osobní údaje o zdravotním stavu. Tak například podle ustanovení § 105 zákoníku práce zaměstnavatele vede v knize úrazů evidence o všech úrazech, i když jimi nebyla způsobena pracovní neschopnost nebo byla způsobena pracovní neschopnost nepřesahující 3 kalendářní dny, a také je povinen vyhotovovat záznamy a vést dokumentaci o všech pracovních úrazech, jejichž následkem došlo ke zranění zaměstnance s pracovní neschopností delší než 3 kalendářní dny, nebo k úmrtí zaměstnance. Rovněž tak je povinen vést evidenci zaměstnanců, u nichž byla uznána nemoc z povolání, která vznikla na jeho pracovištích. Tedy jinak řečeno, jsou zpracovávány informace o zdravotním stavu, a to v souvislosti s pracovním úrazem nebo nemocí z povolání. Že se o citlivé údaje bezpochyby jedná, vyplývá z povahy údajů samotných. Při striktním výkladu pojmu „údaj o zdravotním stavu“ by bylo také možné dovodit, že citlivým osobním údajem je i negativní informace o způsobilosti zaměstnance vykonávat některé činnosti. Jedná se tedy o informaci o zdravotním stavu, neboť důvody pro nevydání například zdravotního průkazu, který je nezbytný pro výkon některých činností, vyplývající ze zvláštního právního předpisu⁴⁸ jsou velmi specifické.

Zaměstnavatelé vedou také ještě další evidence, při nichž dochází ke zpracování osobních údajů. Za všechny lze zmínit například evidenci a vedení dokumentace o školeních o právních a ostatních předpisech k zajištění bezpečnosti a ochrany zdraví při práci podle § 103 odst. 2 a 3 zákoníku práce nebo může vést evidenci o tom, komu a jaké vydal ochranné pracovní prostředky, mycí, čistící a dezinfekční prostředky a ochranné nápoje, jak mu ukládá § 104 odst. 5 zákoníku práce. Takovými evidencemi jsou však také evidence podle jiných zákonů, například vedené pro účely nemocenského a důchodového pojištění, tedy podle zákona č. 582/1991 Sb., o organizaci a provádění sociálního pojištění.

Pro úplnost je třeba ještě zmínit zvláštní právní úpravy týkající se tzv. služebních poměrů. Jedná se například o příslušníky bezpečnostních sborů, tedy o příslušníky Policie České republiky, Hasičského záchranného sboru České republiky, Celní správy České republiky, Vězeňské služby České republiky, Bezpečnostní informační služby a Úřadu pro zahraniční styky a informace. Zvláštní právní úpravu mají také vojáci z povolání.

⁴⁸ Zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, v platném znění.

Zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů (dále jen „služební zákon“), obsahuje právní úpravu, která je z hlediska zpracování osobních údajů ve srovnání se zákoníkem práce mnohem ucelenější a do značné míry přesnější. V § 202 citovaného zákona jsou zakotvena základní pravidla nakládání s osobními údaji a dokumenty, které musí obsahovat osobní spis příslušníka bezpečnostního sboru. Ani zde např. není zmíněna fotografie, jejíž vedení je i z hlediska obecné úpravy zákoníku práce do značné míry výkladovým, a i aplikačním problémem, ale je zde např. jednoznačně stanovena doba uchování osobních údajů, resp. osobního spisu (50 let).

Obdobnou právní úpravu obsahuje také zákon č. 221/1999 Sb., o vojácích z povolání, ve znění pozdějších předpisů, a to v ustanovení § 2a. Je signifikantní, že obě uvedené právní úpravy označují příslušný paragraf rubrikou „osobní údaje“ a obě odkazují ve věcech v nich neupravených na zákon o ochraně osobních údajů. Představují tak zvláštní právní úpravu, kterou je třeba považovat za konformní se zákonem o ochraně osobních údajů, a zpracování osobních údajů na základě citovaných ustanovení je z hlediska zákona o ochraně osobních údajů zpracováním podle § 5 odst. 2 písm. a), podle kterého lze osobní údaje zpracovávat bez souhlasu subjektu údajů, neboť se bude jednat o zpracování nezbytné pro dodržení právní povinnosti správce.

Zvláštní právní úpravu obsahuje také zákon č. 234/2014 Sb., o státní službě, a to poměrně obsáhle. Tak např. podle § 180 se zřizuje informační systém o státní službě jako informační systém veřejné správy, jehož účelem je vedení údajů nezbytných pro správu organizačních věcí služby a služebních vztahů v rámci služebních úřadů i mezi nimi a činění některých úkonů podle tohoto zákona a správcem informačního systému o státní službě je Ministerstvo vnitra. Součástí informačního systému o státní službě je rejstřík státních zaměstnanců, evidence obsazovaných služebních míst, portál pro přihlašování na úřednickou zkoušku a evidence uskutečněných úřednických zkoušek. Podle § 181 je součástí rejstříku velký rozsah osobních údajů státních zaměstnanců a § 182 upravuje značně podrobně i přístupy do tohoto rejstříku.

Lze tedy uzavřít, že všechny výše uvedené evidence a zpracování provádí zaměstnavatel na základě povinností stanovených mu zákonem. Bude se tedy jednat o zpracování, které je možné vykonávat bez souhlasu zaměstnance, a to na základě ustanovení § 5 odst. 2 písm. a) zákona o ochraně osobních údajů, neboť se jedná o zpracování nezbytné pro dodržení právní povinnosti správce, a také nebude třeba pro

taková zpracování plnit oznamovací povinnost podle § 16 zákona o ochraně osobních údajů, neboť v tomto případě bude platit ustanovení § 18 odst. 1 písm. b), které stanoví, že oznamovací povinnost se nevztahuje na zpracování osobních údajů, které správci ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona.

4.6 Předávání osobních údajů do zahraničí

Specifickým problémem, který musí řada zaměstnavatelů jakožto správců osobních údajů řešit, je skutečnost, že v některých případech hodlají předat osobní údaje svých zaměstnanců do zahraničí. Obecně lze říci, že důvody mohou být prakticky jen dva. Může se jednat o předání za účelem (technického) zpracování údajů, které by jinak zaměstnavatel – správce osobních údajů činil sám, anebo za účelem jejich dalšího využití nebo pro potřeby jiného subjektu v zahraničí.

Pravidla předávání osobních údajů do zahraničí obsahuje § 27 zákona o ochraně osobních údajů. Tato pravidla stanoví pro předávání několik různých východisek, na nichž závisí, zda lze osobní údaje do zahraničí předávat volně, tedy bez administrativních překážek, nebo zda je k takovému předání nutné povolení ÚOOÚ. Především platí pravidlo uvedené v odst. 1 citovaného ustanovení, tedy volný pohyb osobních údajů nemůže být omezován, pokud jsou údaje předány do členských států Evropské unie. To znamená, že osobní údaj lze zcela volně v rámci EU předávat bez dalšího omezení a není tedy třeba Úřad žádat o povolení. Obdobný režim platí i pro některé jiné země, které nejsou členskými státy EU, avšak za splnění zvláštní podmínky. Tato podmínka, resp. podmínky vyplývají z ustanovení odst. 2 citovaného zákona § 27 zákona o ochraně osobních údajů, ten stanoví, že do třetích zemí mohou být osobní údaje předány, pokud zákaz omezování volného pohybu osobních údajů vyplývá z mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas a kterou je Česká republika vázána, nebo jsou osobní údaje předány na základě rozhodnutí orgánu Evropské unie. Takovou smlouvou je např. Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (Rada Evropy, ETS 108, 1981). Právní předpisy zemí⁴⁹ (členské státy EU v to nepočítaje), které k této smlouvě přistoupily,

⁴⁹ V současné době např. Albánie, Bosna a Hercegovina, Černá Hora, Gruzie, Chorvatsko, Island, Lichteštejnsko, Makedonie, Moldavsko, Norsko, Srbsko, Švýcarsko, Andorra nebo také Mauritius, Marocco, Senegal a další. Úplný přehled je uveden na <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>.

totiž zaručují dostatečnou ochranu osobních údajů odpovídající všem požadavkům směrnice Evropského parlamentu a Rady 95/46/ES.

Druhou skupinou tzv. třetích zemí, do nichž je možné předávat osobní údaje bez povolení Úřadu, tvoří ty země, o nichž jakožto o zemích bezpečných z hlediska ochrany zpracování osobních údajů rozhodl příslušný orgán (Komise) Evropské unie⁵⁰. Specificky je nutno přistupovat k předávání osobních údajů do USA a Kanady. V případě těchto států závisí na konkrétním posouzení uvažovaného předání, zda jsou v daném případě splněny podmínky stanovené rozhodnutím orgánu EU. V tomto případě lze doporučit, aby takové předání bylo před jeho realizací minimálně konzultováno s Úřadem.

Nejedná-li se o výše uvedené případy, je nutné v souladu s ustanovením § 27 odst. 4 zákona o ochraně osobních údajů před předáním osobních údajů do třetích zemí požádat Úřad o povolení k předání (nestanoví-li zvláštní zákon jinak). Při posuzování žádosti Úřad přezkoumá všechny okolnosti související s předáním osobních údajů, zejména zdroj, konečné určení a kategorie předávání osobních údajů, účel a dobu zpracování, s přihlédnutím k dostupným informacím o právních nebo jiných předpisech upravujících zpracování osobních údajů ve třetí zemi. V povolení k předání, které je rozhodnutím ve smyslu správního řádu, Úřad stanoví dobu, po kterou může správce předání provádět. Pokud dojde ke změně podmínek, za kterých bylo povolení vydáno, zejména na základě rozhodnutí orgánu EU, Úřad toto povolení změní nebo zruší. Důvody, pro které je možno žádat Úřad o povolení k předání osobních údajů, pak stanoví § 27 odst. 3 zákona o ochraně osobních údajů s tím, že takové důvody budou prokazatelné. To znamená, že v žádosti o předání by měl zaměstnavatel, který hodlá osobní údaje předat či předávat do třetích zemí, prokazatelně doložit, že v daném případě se jedná o některý z důvodů uvedených v citovaném ustanovení, tedy že:

- a) předání údajů se děje se souhlasem nebo na základě pokynu subjektu údajů,
- b) jsou v třetí zemi, kde mají být osobní údaje zpracovány, vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, například prostřednictvím jiných právních nebo profesních předpisů a bezpečnostních opatření. Takové záruky mohou být upřesněny zejména smlouvou uzavřenou mezi správcem a příjemcem, pokud tato smlouva zajišťuje uplatnění těchto požadavků nebo

⁵⁰ V současné době se jedná o Argentinu, Faerské ostrovy, Guernsey, Jersey, Nový Zéland, Ostrov Man, Švýcarsko, Izrael, Andorrské knížectví, Uruguay.

pokus smlouva obsahuje smluvní doložky pro předání osobních údajů do třetích zemí zveřejněné ve Věstníku Úřadu,

- c) jde o osobní údaje, které jsou na základě zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem, v takovém případě lze osobní údaje zpřístupnit jen v rozsahu a za podmínek stanovených zvláštním zákonem,
- d) je předání nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo z mezinárodní smlouvy, kterou je Česká republika vázána,
- e) je předání nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů,
- f) je předání nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou, nebo pro uplatnění jiných právních nároků, nebo
- g) je předání nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů, zejména pro záchranu života nebo pro poskytnutí zdravotních služeb.

Je však třeba mít na paměti, že problematika předávání zaměstnaneckých údajů do zahraničí je limitována nejen podmínkami stanovenými v § 27 zákona o ochraně osobních údajů, ale také skutečností, že zpracování zaměstnaneckých údajů musí být v souladu s dalšími požadavky zákona o ochraně osobních údajů, neboť se bude jednat často o zpracování osobních údajů, resp. činnosti upravené zvláštními předpisy. Zpracování pak musí být také v souladu s pravidly v těchto předpisech uvedenými, přičemž na tato pravidla je nutno pohlížet jako na upřesnění zásad ochrany osobních údajů stanovených v zákoně o ochraně osobních údajů. Nemělo by tedy docházet ke „quasilegálnímu“ předávání osobních údajů pro takové zpracování v zahraničí, které je však v rozporu s podmínkami takového zpracování požadovanými právním řádem České republiky (předpisy a rozhodnutí orgánů EU).

V případě posuzování pracovního práva jako odvětví soukromého práva je nutno konstatovat, že v daném případě jsou účel a případné meze nakládání se zaměstnaneckými údaji stanoveny právními předpisy.

Osobní údaje zaměstnanců neslouží jen k zajištění trvání pracovněprávního vztahu zaměstnance k zaměstnavateli, ale mohou být také podkladem pro jiné činnosti, např. pro vyhodnocení racionalizace práce, efektivity činností a trendů dalšího vývoje

zaměstnavatele. V tomto případě však nastává nutnost osobní údaje zaměstnance před předáním anonymizovat, neboť dochází ke zpracování údajů, jehož účelem je zajištění hospodářských cílů zaměstnavatele. Zpracováním neanonymizovaných dat, která se sice mohou dotýkat zaměstnance, ale v první řadě bezprostředně slouží ekonomickým potřebám zaměstnavatele, je zjevně překračován rámec (účel) právními předpisy stanoveného nakládání s osobními údaji zaměstnanců.

V řadě případů předávání osobních údajů do jiných států je požadavek jejich zpracování dán specializovanými či odbornými pracovišti u tzv. mateřských společností v zahraničí, které jsou z pohledu zákona o ochraně osobních údajů zpracovatelem. Pak je nutné naplnit zejména ustanovení § 6 zákona o ochraně osobních údajů, tedy uzavřít smlouvu mezi správcem a zpracovatelem. Uvedený zpracovatel však není oprávněn předmětné osobní údaje zpracovávat pro jiné účely a pro jiné správce (pro uvedené účely je však možné údaje anonymizovat). Často také dochází k předávání osobních údajů do zahraničí pro přípravu a realizaci vzdělávacích programů některých skupin zaměstnanců a v případech jejich vysílání na pracovní cesty do zahraničí. V takovém případě je obvykle naplněna některá z podmínek § 27 zákona o ochraně osobních údajů, když je např. nezbytné respektovat předpisy o pobytu cizinců v dané zemi. Pokud však zaměstnavatel v souvislosti s vysláním zaměstnance do zahraničí, obvykle z důvodu dlouhodobějšího pobytu zaměstnance (a případně i jeho rodinných příslušníků), zpracovává osobní údaje členů rodiny zaměstnance, je nezbytné získat souhlasy subjektů k takovému zpracování⁵¹.

V souvislosti s předáváním osobních údajů do třetích zemí je třeba ještě upozornit na dva zvláštní instituty, které jsou z hlediska předávání praktické a jejichž význam bude pravděpodobně stoupat. Jedná se o tzv. Standardní smluvní doložky a také o „Závazná podniková pravidla“ (Binding Corporate Rules) jako nástroje bezpečného předávání osobních údajů do třetích zemí.

Standardní smluvní doložky jsou nástrojem, který je považován za dostatečné ochranné opatření s ohledem na ochranu soukromí a základních práv a svobod jednotlivců, jakož i s ohledem na výkon odpovídajících práv v souladu s čl. 26 odst. 2 Směrnice 95/46/ES. Tyto smluvní doložky jsou vydávány ve formě rozhodnutí Komise

⁵¹*Předávání osobních údajů do zahraničí*, [online]. Praha, UOOU, 2010. Dostupné z WWW: <<http://uouu.cz/predavani-osobnich-udaju-zamestnancu-do-zahranici/ds-1655>>.

(ES) a v současné době jsou vydána taková rozhodnutí tři⁵². Jejich význam spočívá v tom, že při jejich použití má zaměstnavatel, tedy správce osobních údajů, jistotu, že ochrana předaných nebo předávaných údajů bude odpovídat evropskému standardu. Současně však platí, že doložky, jejichž text byl publikován ve Věstníku Úřadu a je přístupný i na jejich webových stránkách, musí být použit tak, jak byl Komisí schválen a nelze ne jejich textu nic měnit. Jednotlivá ustanovení doložek nelze ani kombinovat mezi sebou. Lze však zvolit typ doložky, který bude správci při předávání lépe vyhovovat, resp. bude odpovídat charakteru předání a jeho účelu.

Další možností pro předávání osobních údajů do zahraničí, resp. do třetích zemí je, že osobní údaje mohou být předány pouze za předpokladu, že dotyčná třetí země zajistí odpovídající úroveň ochrany, a v případě předání osobních údajů do třetí země, která nezajišťuje odpovídající úroveň ochrany, může být takové předání uskutečněno, i pokud náležitá opatření směřující k ochraně osobních údajů poskytne sám správce. Jednou z možností, jak lze zajistit ochranu a legálnost zpracování a přenosu osobních údajů do třetích zemí, je přijetí „Závazných podnikových pravidel“ (Binding Corporate Rules). Tento způsob je vhodný zejména pro velké nadnárodní společnosti, neboť Závazná podniková pravidla (ZPP) pro ně představují nejschůdnější a nejlevnější cestu k legálnímu zpracování a přenosu dat v rámci celé společnosti. V této souvislosti je nutné zdůraznit, že ZPP platí pouze pro přenos osobních údajů v rámci jedné nadnárodní společnosti, nikoli již pro předání mimo tuto společnost. Pro tyto případy (tzv. onward transfer) je možné použít např. standardní smluvní doložky. Společnost, která se rozhodne zavést ZPP, se mj. musí zavázat, že stanovená pravidla ochrany osobních údajů budou přijata v celé společnosti (tedy všemi organizačními složkami) a že bude zajištěno jejich dodržování prostřednictvím zavedených dozorových mechanismů. Skutečná závaznost, tj. vymahatelnost přijatých principů, je jedním z hlavních závazků a zároveň „stavebním kamenem“ každých ZPP. I když je skutečností, že vytvoření a konečné schválení ZPP je poměrně složitý a časově náročný

⁵² Pro případ předání osobních údajů zpracovateli osobních údajů do třetích zemí jsou určeny standardní smluvní doložky, které jsou přílohou Rozhodnutí Komise ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelů usazených ve třetích zemích podle směrnice 95/46/ES. Pro případ předání osobních údajů novému správci osobních údajů do třetích zemí lze použít buď standardní smluvní doložky obsažené v Rozhodnutí Komise ze dne 15. června 2001 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle směrnice 95/46/ES, nebo standardní smluvní doložky obsažené v Rozhodnutí Komise ze dne 27. prosince 2004, kterým se mění rozhodnutí 2001/497/ES, pokud jde o zavádění alternativního souboru standardních smluvních doložek pro předávání osobních údajů do třetích zemí.

proces, jeho absolvování se řadě velkých korporací jistě vyplatí, neboť tak eliminují rizika plynoucí z neoprávněného zpracování (předávání) osobních údajů⁵³.

4.7 Zpracování osobních údajů po ukončení pracovního poměru

Uchování osobních údajů zaměstnanců po skončení pracovního poměru zákoníku práce přímo nikterak neřeší, i když je tato problematika zaměstnavateli často traktována. Z pohledu zákona o ochraně osobních údajů, který uchovávání osobních údajů uvádí v § 4 písm. e) jako jednu z forem zpracování a samo uchovávání pak definuje v písm. g) téhož ustanovení jako udržování údajů v takové podobě, která je umožňuje dále zpracovávat, je třeba tuto problematiku vyjasnit minimálně z důvodu ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů, které stanoví obecnou povinnost uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné.

Dobou nezbytnou pro zpracování osobních údajů zaměstnanců je z povahy věci obecně doba, po kterou trvá pracovní nebo jiný obdobný poměr. Rozsah údajů zpracovávaných pro účely pracovního poměru v osobním spisu zaměstnance a v jiných evidencích zaměstnavatele je limitován svým obsahem na údaje, resp. písemnosti bezpochyby osobní údaje obsahující, které jsou nezbytné pro výkon práce v pracovněprávním vztahu (§ 312 odst. 1 zákoníku práce). Po ukončení pracovněprávního nebo jiného obdobného vztahu je možno osobní údaje uchovávat jen z důvodů, které jsou stanoveny v právním předpise. Vodítko, o jaké informace (osobní údaje) se jedná, poskytuje ustanovení § 150 zákoníku práce. Ten stanoví, že zaměstnavatel eviduje údaje, jimiž jsou jméno, popřípadě jména a příjmení, adresa, jde-li o fyzickou osobu, název a sídlo, jde-li o právnickou osobu, a písemnosti týkající se prováděných srážek ze mzdy, a to po stejnou dobu jako ostatní údaje a doklady týkající se mzdy nebo platu a odkazuje na zvláštní zákon, kterým je zákon č. 499/2004 Sb., o archivnictví a o spisové službě a o změně některých zákonů, ve znění pozdějších

⁵³*Předávání osobních údajů do zahraničí – Závazná podniková pravidla (Binding Corporate Rules).* Dostupné na <https://www.uouu.cz/zavazna-podnikova-pravidla-binding-corporate-rules-bcr/ds-3506/pl=3506>

předpisů. Okruh povinných osob, uvedených v § 3 citovaného zákona, zahrnuje většinu zaměstnavatelů, avšak přesné určení, které z dokumentů a jak dlouho se mají uchovávat, nestanoví a nečiní tak ani prováděcí právní předpisy⁵⁴.

Jedním z právních předpisů, kterým jsou stanoveny uschovací lhůty pro uchovávání některých vybraných dokumentů, je například zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení. Ten stanoví řadu uschovacích lhůt např. v ustanovení § 35a odst. 4 tak, že zaměstnavatelé jsou povinni uchovávat:

- a) stejnopisy evidenčních listů (§ 38 odst. 5 věta první) vyhotovených v kalendářním roce, kterého se týkají, nebo v bezprostředně následujícím kalendářním roce po dobu 3 kalendářních roků po roce, kterého se týkají, a stejnopisy ostatních evidenčních listů po dobu 3 kalendářních roků po roce, ve kterém byly vyhotoveny,
- b) záznamy o skutečnostech vedených v evidenci podle § 37 odst. 1 písm. h) po dobu 6 kalendářních roků následujících po měsíci, kterého se záznam týká, vždy však po dobu 3 kalendářních roků následujících po měsíci, v němž bylo dlužné pojistné za tento měsíc zapláceno,
- c) záznamy o skutečnostech vedených v evidenci podle § 37 odst. 1, pokud jde o poživatele starobního nebo invalidního důchodu, po dobu 10 kalendářních roků po roce, kterého se týkají,
- d) mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění, včetně údajů uvedených v § 37 odst. 2, po dobu 30 kalendářních roků následujících po roce, kterého se týkají, a jde-li o mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění vedené pro poživatele starobního důchodu, po dobu 10 kalendářních roků následujících po roce, kterého se týkají, pokud zvláštní právní předpis nestanoví pro záznamy, které mají charakter účetních záznamů, delší uschovací dobu, za záznamy o těchto skutečnostech se vždy považují doklady druhu, vzniku a skončení pracovního vztahu, záznamy o pracovních úrazech a o nemocech z povolání a záznamy o evidenci pracovní doby včetně doby pracovního volna bez náhrady příjmu.

⁵⁴ Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých předpisů. Vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby.

Takto stanovené uschovací lhůty jsou tedy dobou, po kterou je nezbytné zpracovávat (uchovávat) osobní údaje zaměstnanců i po skončení pracovního poměru. De facto jsou tak stanoveny i druhy dokumentů, které uchovány být musí. Je zjevné, že mezi uchovávané dokumenty nepatří např. životopis nebo různá osvědčení, která zaměstnanec zaměstnavateli předložil v době trvání pracovního poměru a která po jeho skončení pro zaměstnavatele ztratila relevanci. Takové dokumenty by měly být zaměstnanci vráceny nebo prokazatelně zlikvidovány, neboť jen tak bude u posledně zmíněných dokumentů naplněno ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů, tedy že správce (zaměstnavatel) je povinen uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování.⁵⁵

5 Empirická část

V poslední části této bakalářské práce byla uplatněna metoda polostrukturovaných rozhovorů. V časovém období od 1. 10. 2017 do 31. 1. 2018 probíhaly rozhovory se zaměstnanci, tyto rozhovory měly odpovědět na otázku, v jakém stavu je nakládání s osobními údaji zaměstnanců výrobní společnosti XY. Rozhovory byly zacílené na aplikaci zákonných požadavků ochrany osobních údajů z pohledu personálního oddělení (HR), aplikaci ochranných prvků v systémech zpracovávání a uchovávání osobních údajů z pohledu technického zajištění oddělení Informační technologie (IT) a v poslední řadě informace od kmenových zaměstnanců. Rozhovory byly provedeny s 96 zaměstnanci, a žádný z celé skupiny si nepřeje být jmenován. Kompetentní zaměstnanci z oddělení HR a IT byli k rozhovoru vybráni na základě jejich pracovní náplně. Rozhovory probíhaly mimo prostory společnosti mimo jejich pracovní dobu a vždy v přátelské uvolněné atmosféře.

5.1 Analýza informací

Představení společnosti XY

Jedná se o zahraniční společnost s ručením omezeným, která na Vysočině působí skoro 20 let. Tato společnost patří do segmentu „automotive“ a produkuje výrobky, které používají auta na celém světě. V současné době zaměstnává 1000 pracovníků a patří mezi významné zaměstnavatele v regionu.

⁵⁵ BARTÍK, V., JANEČKOVA, E. *Ochrana osobních údajů v aplikační praxi*, Praha 2016, s. 175

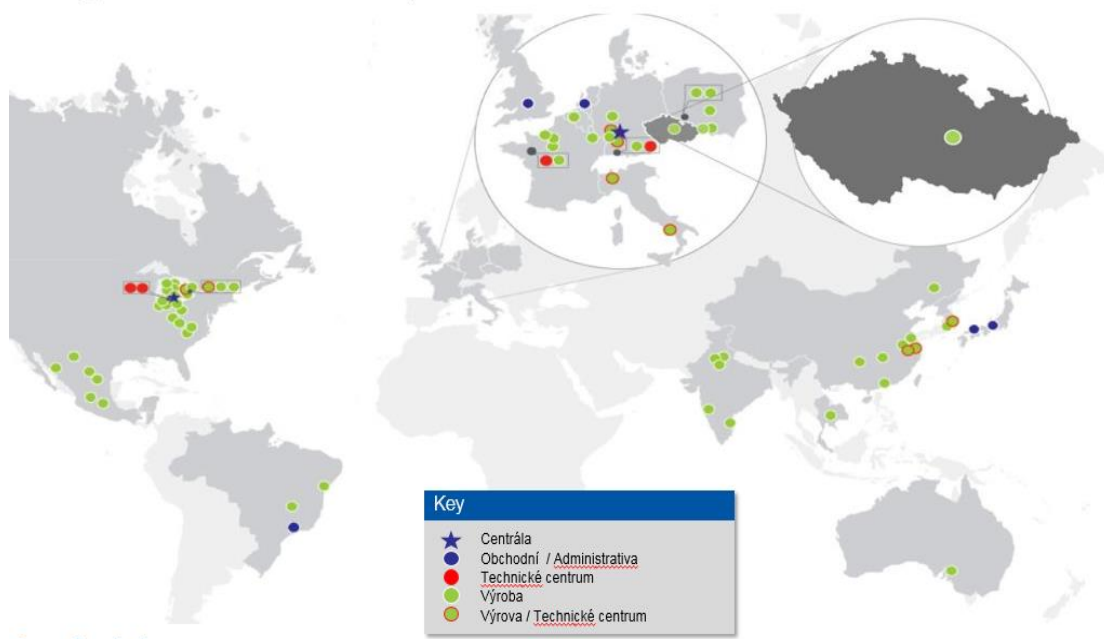
Obr. č.: 1 Informace o společnosti

Informace o společnosti

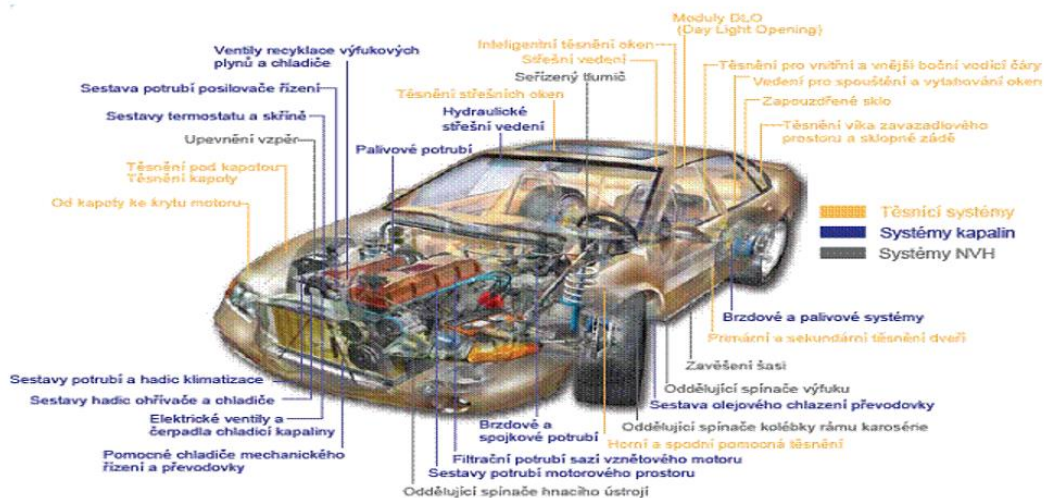


Obr. č.: 2 Organizační členění společnosti

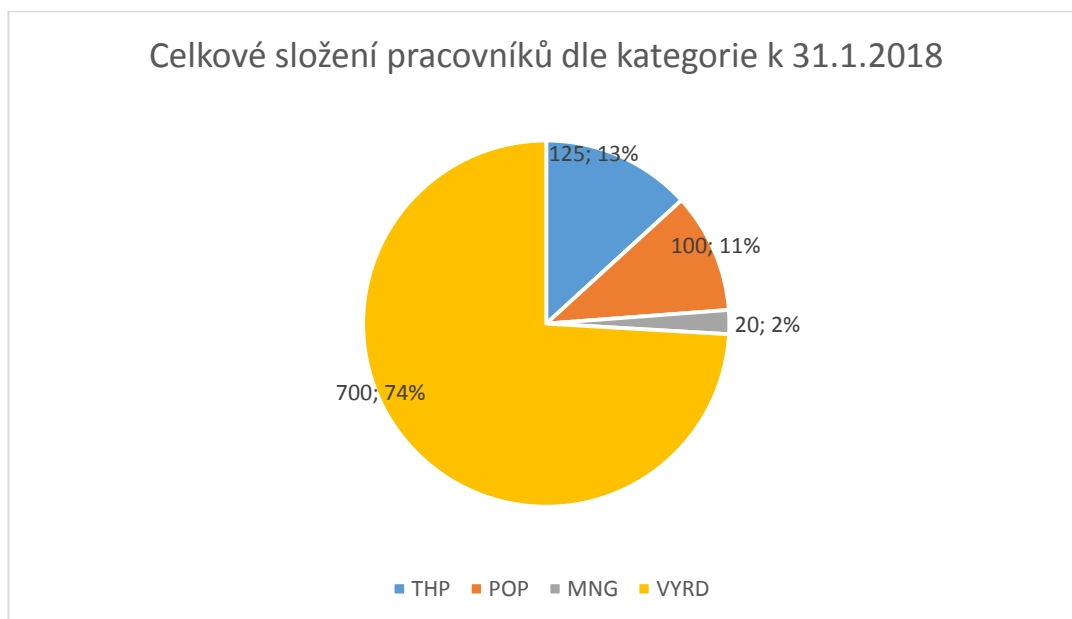
Organizační členění společnosti



Produkty společnosti



Graf.č.1: Složení společnosti dle kategorie pracovníků



K výzkumnému šetření bylo využito metody pokládání jednoduchých otázek „face to face“. Zároveň zde byl nechán prostor na otázky s možností otevřených odpovědí.

Graf č. 2 Pracovní pozice účastníků ověřování



5.1.1 Hypotézy

Hypotéza č. 1: Předpokládám, že nastavení požadavků a kontrolních mechanismů z pohledu HR a IT je dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů a Nařízení EU 2016/679 (GDPR)

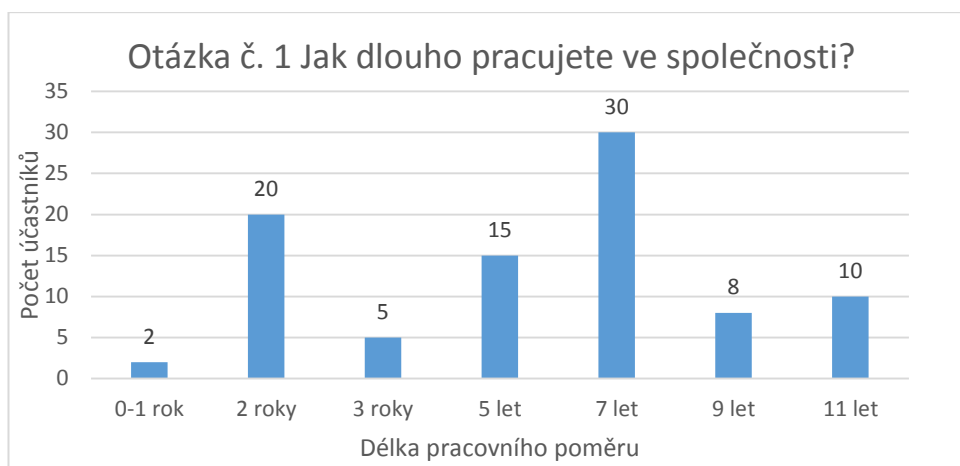
Hypotéza č. 2: Předpokládám, že pracovníci jsou řádně informováni a seznamováni s ustanovením zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů a Nařízení EU 2016/679 (GDPR)

5.1.2 Vyhodnocení rozhovorů

Otázka č.: 1: Jak dlouho pracujete ve společnosti?

Většina respondentů pracuje ve společnosti delší dobu. Pouze 2 % pracovníků, kteří se zúčastnili těchto rozhovorů, pracuje ve společnosti do 1 roku.

Graf č. 3: Otázka č. 1 Jak dlouho pracujete ve společnosti?

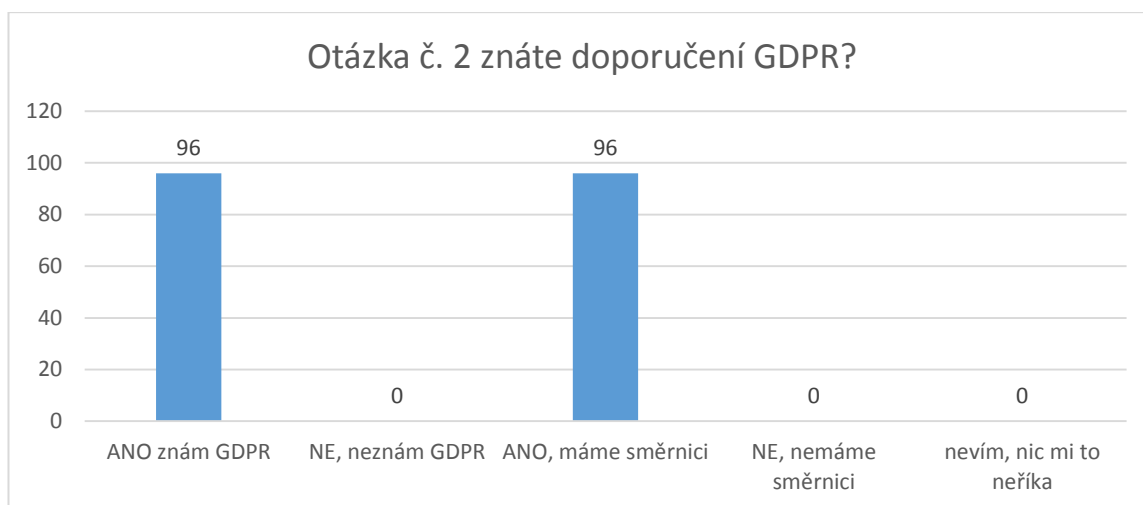


**Otázka č.: 2: Znáte doporučení GDPR na správu a zabezpečení osobních údajů?
Pokud ano, jsou ve společnosti aplikovány?**

Pracovníci oddělení HR i IT shodně odpověděli, že ano, doporučení a celá problematika ochrany osobních údajů a GDPR je jim známa. Od loňského roku se účastnili několika školení a v rámci svých oddělení aktualizovali směrnici na tyto postupy.

Více jak polovina dotázaných si nebyla jistá se zkratkou GDPR, ale po vysvětlení, že se jedná o ochranu osobních údajů, které poskytují zaměstnavateli, reagovali všichni tím, že znají a jsou informováni. Všichni potvrdili, že „směrnice“ jak postupovat při sdělování osobních údajů existuje, jsou s ní seznámeni a je dodržována. Pracovníci znali postup udělování souhlasu s použitím osobní fotografie ve firemním časopise, znali postup, jak požádat o zrušení uděleného souhlasu. Celá skupina potvrdila, že personální oddělení (HR) prováděla v loňském roce rozsáhle školení, kde byli s touto problematikou řádně seznámeni. Dokonce, i že je to součást opakovacího školení na pracovišti.

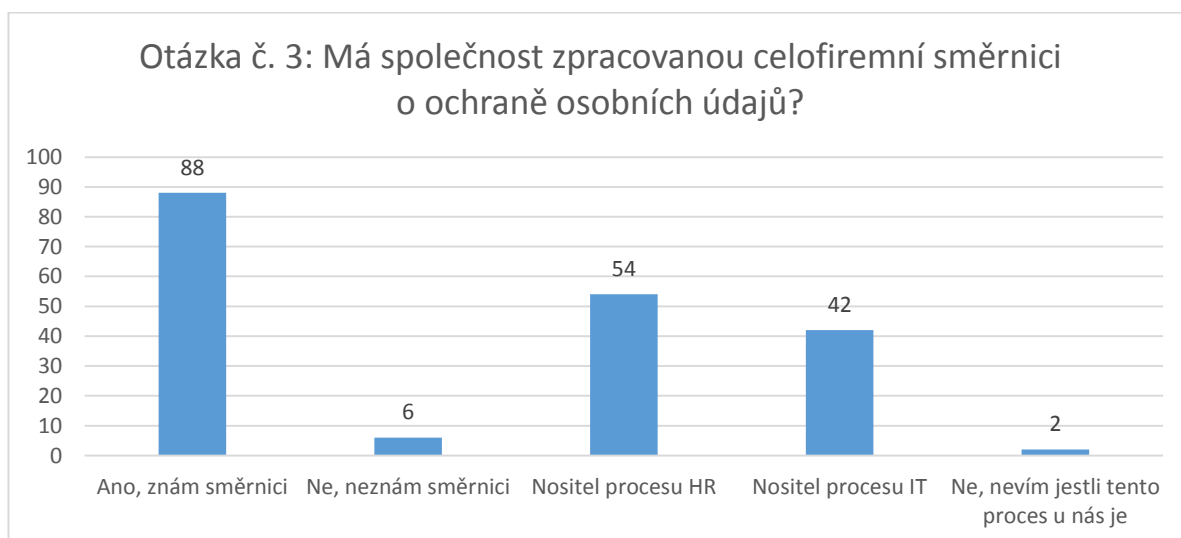
Graf č.: 4 Otázka č. 2: znáte doporučení GDPR?



Otázka č.: 3: Máte zpracovanou celofiremní směrnici na práci a ochranu s osobními údaji? Pokud ano, kdo je nositelem tohoto procesu a proč?

Z odpovědi na tuto otázku vyplynulo, že ve společnosti je zpracovaná směrnice na ochranu osobních údajů a jsou v ní zahrnuty odpovědnosti napříč celou společností. Nositelem tohoto procesu je personální oddělení. A to z důvodu, že většina jak pracovníků, tak i respondentů tohoto dotazování si myslí, že největší díl osobních údajů zpracovává právě HR oddělení. Ve výzkumném vzorku byli 2 pracovníci HR oddělení a i oni s tímto názorem souhlasili.

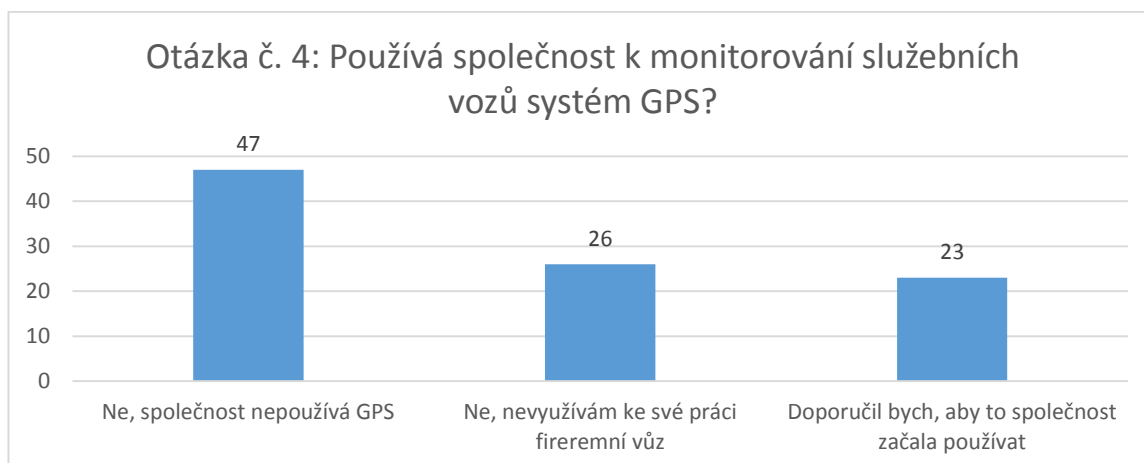
Graf č. 5 Otázka č. 3 Má společnost zpracovanou celofiremní směrnici o ochraně osobních údajů?



Otázka č.4: Používá společnost k monitorování používání služebních vozů systém GPS?

Ne, společnost nepoužívá k monitorování používání služebních vozů žádný systém, a tedy ani GPS. Přidělování služebních vozů tzv. „manažerských“ řeší v celofiremní předpisu „Policy car“, a využívání tzv. referentských vozidel probíhá na základě schválené služební cesty na řízeném formuláři – Cestovní příkaz. Přesto velká část respondentů by se přikláněla k používání některého z elektronického systému, hlavně z důvodu evidence jízd, která je v dnešní době prováděna formou papírové knihy jízd. Hlavně by respondenti uvítali elektronický systém na rezervaci firemních vozů, protože se stále častěji potýkají s nedostatkem služebních vozů než s tím, že by systém GPS mohl ohrozit jejich soukromí.

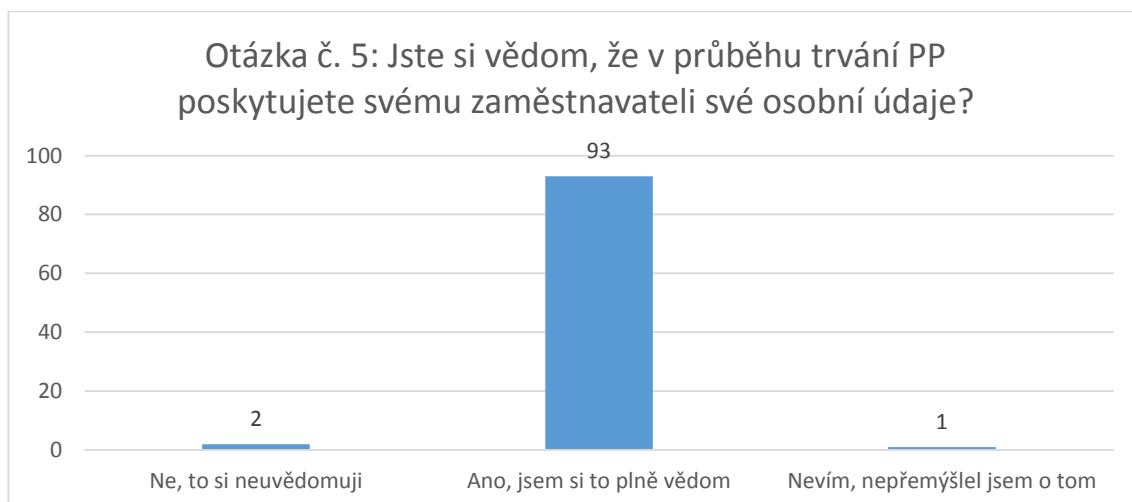
Graf č. 6 otázka č. 4 Používá společnost k monitorování služebních vozů systém GPS?



Otázka č. 5: Jste si vědom, že v průběhu trvání pracovního poměru poskytl jste svému zaměstnavateli své osobní údaje?

Z výsledku je patrné, že skoro všichni respondenti si jsou vědomi, že poskytují svoje aktuální osobní údaje po celou dobu trvání pracovního poměru. Pracovníci společnosti se v nedávné době účastnili školení na ochranu osobních údajů, kde byli seznámeni se základní informací jak společnost nakládá s informací, kterou jí poskytne zaměstnanec, a pokud by tento průzkum probíhal s větším časovým odstupem mohl by být tento výsledek úplně jiný.

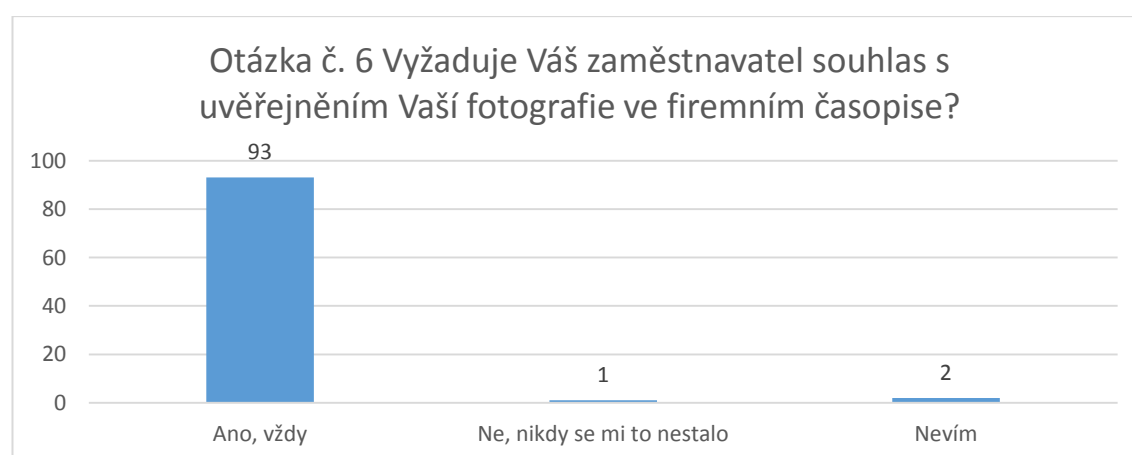
Graf č. 7 otázka č. 5 Jste si vědom, že v průběhu trvání pracovního poměru poskytlujete svému zaměstnanci své osobní údaje?



Otázka č. 6 Vyžaduje Váš zaměstnavatel souhlas s uveřejněním Vaší fotografie ve firemním časopise?

Společnost vydává svůj vlastní časopis, kde uveřejňuje fotografie z výroby, firemních akcí a také fotografie pracovníků k životním nebo pracovním výročím. Pouze necelá 3 % respondentů uvedla, že o souhlasu neví, nebo že není vyžadován.

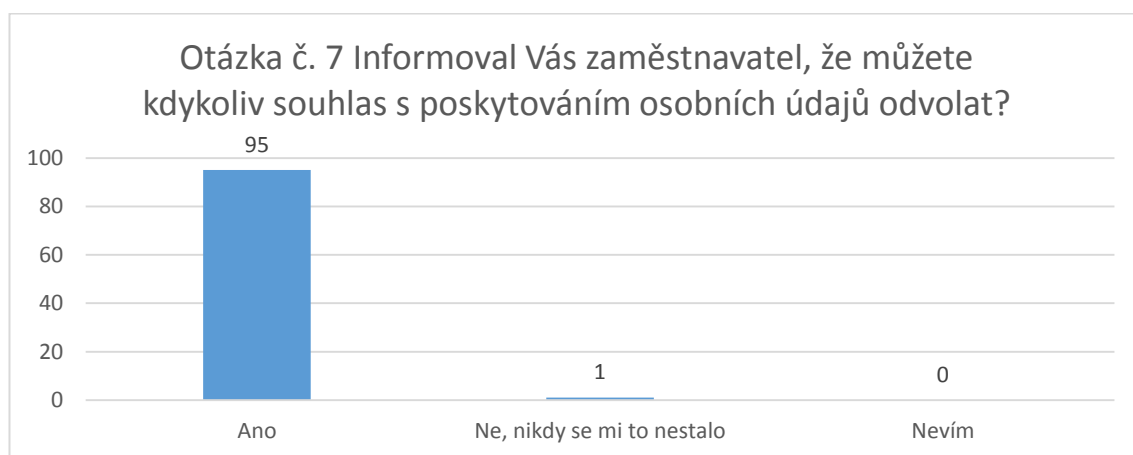
Graf č. 8: Otázka č. 6 Vyžaduje Váš zaměstnavatel souhlas s uveřejněním Vaší fotografie ve firemním časopise?



Otázka č. 7 Informoval Vás zaměstnavatel, že můžete kdykoliv souhlas s poskytováním osobních údajů odvolat?

Dá se říci, že všichni respondenti shodně potvrdili, že jim tato možnost o odvolání souhlasu je známa. V současnosti nikdo této možnosti nevyužil. Je možné i říci, že všichni si vážili toho, že jim bylo vysvětleno, jak se s jejich údaji zachází, a že mají možnost s něčím nesouhlasit.

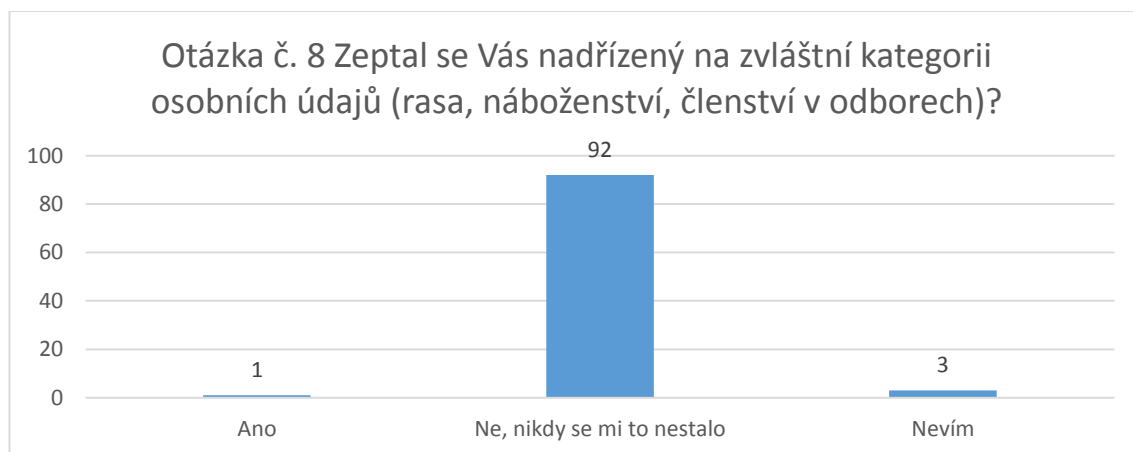
Graf č. 9: Otázka č. 7: Informoval Vás zaměstnavatel, že můžete kdykoliv souhlas s poskytováním osobních údajů odvolat?



Otázka č. 8: Zeptal se Vás nadřízený na zvláštní kategorii osobních údajů?

Výsledek, u této odpovědi, je trošku zavádějící, nejdříve se muselo respondentům vysvětlit, co je myšleno tou zvláštní kategorií osobních údajů. Pak už bez zaváhání došlo k potvrzení, že se nikdo ve společnosti na tyto osobní údaje neptá.

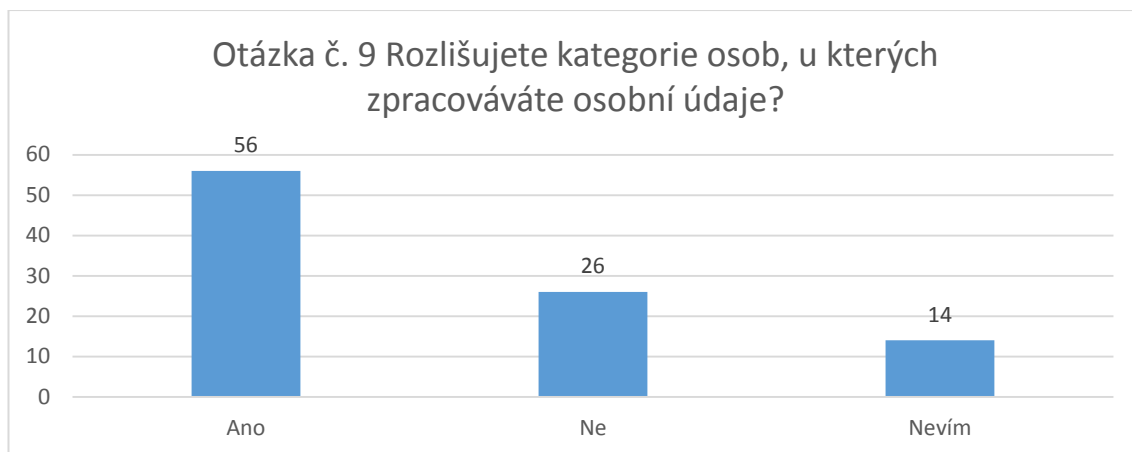
Graf č. 10: Otázka č. 8: Zeptal se Vás nadřízený na zvláštní kategorii osobních údajů?



Otázka č. 9: Rozlišujete kategorie osob, u kterých zpracováváte osobní údaje?

Více jak polovina, celkem 56 respondentů bylo schopno rozlišit základní kategorie osob a popsat rozdíl v rozsahu zpracovávaných osobních údajů.

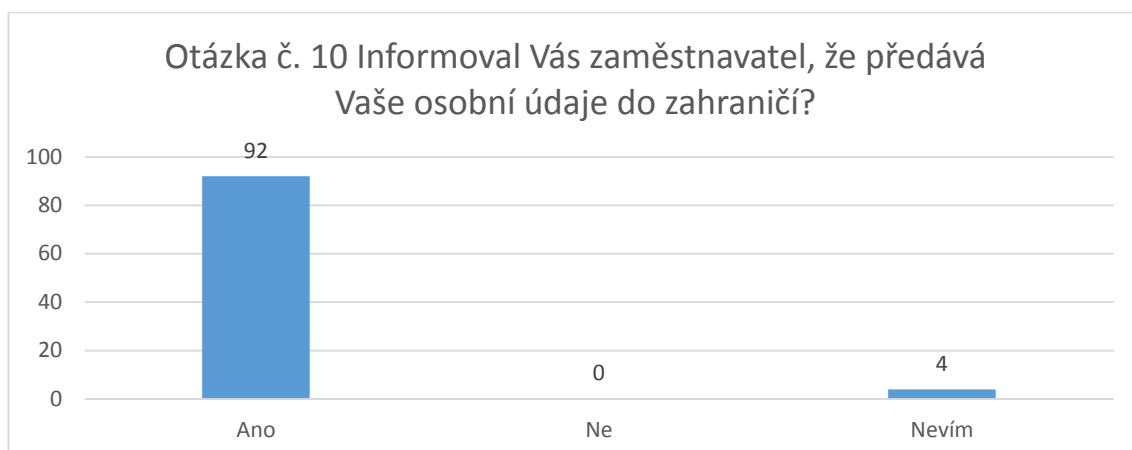
Graf č. 11: Otázka č. 9: Rozlišujete kategorie osob, u kterých zpracováváte osobní údaje?



Otázka č. 10: Informovala Vás společnost, že předává Vaše osobní údaje do zahraničí?

Společnost XY je nadnárodní společnost, a proto většina respondentů počítá s tím, že jejich osobní údaje se odesílají na centrálu. Část pracovníků je zároveň členy mezinárodních týmů řešení například reklamací a sami sdělují svoje informace na pracovních portálech. Přesto je vhodné pracovníky upozornovat, že jejich osobní údaje jsou předávány do zahraničí a jak je s nimi nakládáno dál včetně jejich zabezpečení.

Graf č. 12: Otázka č. 10: Informoval Vás zaměstnavatel, že předává Vaše osobní údaje do zahraničí?



Závěr

Bakalářská práce byla zaměřená na ochranu osobních údajů a nakládání s nimi, a to z pohledu vzniku, trvání a zániku pracovního poměru. U stanovené problematiky bylo důležité nejprve specifikovat základní pojmy jako je osobní údaj, správce, zpracovatel. Jedná se o pojmy ze zákona o ochraně osobních údajů, které jsou pro danou problematiku stěžejní.

Jako další důležitý bod bylo třeba si uvědomit, že nastavení procesu ochrany osobních údajů je podstatnou součástí fungování každé společnosti, že se jedná o náročný proces, pokud tedy chce společnost dodržet všechny zákonné požadavky a zároveň udržet efektivitu vlastní práce. Tento proces není úplně snadný, jak by se někdo mohl domnívat, jedná se o několikvrstvý proces, kdy je podstatné si uvědomit, jaký osobní údaj zpracovávám v souladu se zákonem, tj. musí být založen na jednom ze zákonných důvodů uvedených v GDPR. Legitimní zájem je jedním ze zákonných důvodů.

Obecné nařízení o ochraně osobních údajů (GDPR) nabude účinnosti dne 25. května 2018 a bude v České republice platit namísto dosavadního zákona o ochraně osobních údajů. Nařízení GDPR je z pohledu zaměstnavatele potřeba věnovat zvláštní pozornost, jelikož jeho správný výklad se neobejde bez uvedení do souvislostí se zákoníkem práce a zákonem o zaměstnanosti. Proto je nutné se zaměřovat na pravidla o ochraně soukromí a osobní údaje uchazečů o zaměstnání se zaměřením na vysvětlení toho, které postupy zaměstnavatele jsou bez dalšího přípustné, které jsou podmíněny souhlasem uchazeče o zaměstnání, a které naopak není možné praktikovat, i kdyby k nim uchazeč o zaměstnání dal souhlas.

Základní pravidlo pro získávání informací se nachází v ustanovení § 1 odst. 2 a § 3 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), které obecně stanoví, že zaměstnavatel může činit vše, co je jeho právem nebo oprávněným zájmem, avšak nesmí tím poškodit práva druhé strany nebo porušit výslovný zákaz zákona.

Nepřekročitelnou hranici vymezuje ustanovení § 12 odst. 2 zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (dále jen „zákon o zaměstnanosti“), když zaměstnavateli při výběru zaměstnanců zakazuje vyžadovat

informace týkající se národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení a sexuální orientace. Dále zaměstnavatel nesmí vyžadovat informace, které odporují dobrým mravům, a osobní údaje, které neslouží k plnění povinností zaměstnavatele stanovených příslušnými právními předpisy.

Společnost osobní údaje zpracovává, a proto je dle Obecného nařízení (GDPR) správcem osobních údajů. Interní směrnici si jasně stanovila práva a povinnosti zaměstnanců společnosti a ostatních fyzických osob a fyzických osob podnikajících při veškerém zpracování osobních údajů, a to jak při ručním, tak automatizovaném zpracování. Ke zpracování osobních údajů uvedených subjektů údajů vyžaduje nutný souhlas jednotlivých fyzických osob, ledaže jsou údaje zpracovávány v souladu s článkem 6 odst. 1 písm. b), písm. c) či písm. f) Obecného nařízení (GDPR), tedy z důvodu plnění smlouvy, plnění právní povinnosti nebo oprávněného zájmu. Organizační směrnice coby vnitřní předpis společnosti upravuje postup a zásady jejich zaměstnanců, jakož i dalších pověřených osob při nakládání, zpracování a ochraně osobních údajů zpracovávaných v podmínkách provozu společnosti podle Obecného nařízení (GDPR).

Zaměstnanecká databáze obsahuje osobní údaje zaměstnanců společnosti, a to osobní údaje požadované právními předpisy pro zpracování personálně-mzdové agendy. Osobní údaje jsou zpracovávány v souladu s čl. 6 odst. 1 písm. c) Obecného nařízení (GDPR), tedy z titulu plnění právní povinnosti, za účelem vedení personálně-mzdové agendy. Tyto osobní údaje se zpracovávají po dobu trvání pracovního poměru a dále pak v souladu se zákoníkem práce a právními předpisy týkajícími se sociálního zabezpečení po dobu 3, resp. 10, resp. 30 let a následně se likvidují. Kromě výše uvedených osobních údajů poskytují zaměstnanci společnosti e-mail, telefonní číslo a fotografii, jež společnost zpracovává v souladu s 6 odst. 1 písm. a) na základě souhlasu od subjektu údajů, zaměstnanců společnosti. Stejně tak zaměstnanci poskytují souhlas se zpracováním osobních údajů třetími osobami, konkrétně tzv. sestrami, které jsou společnostmi v rámci koncernu. Osobní údaje, e-mail, telefonní číslo a fotografie se zpracovávají po dobu trvání pracovněprávního vztahu a následně po ukončení pracovněprávního vztahu se likvidují. Dále je ve společnosti databáze pracovních incidentů, jedná se o zákonnou evidenci pracovních úrazů. Tato databáze obsahuje osobní údaje zaměstnanců společnosti, a to údaje požadované právními předpisy v oblasti bezpečnosti a ochrany zdraví při práci, konkrétně se jedná o jméno, příjmení,

datum narození. Osobní údaje v této databázi jsou zpracovávány v souladu s čl. 6 odst. 1 písm. c) Obecného nařízení (GDPR), tedy z titulu plnění právní povinnosti, za účelem vedení evidence pracovních úrazů a evidence zaměstnanců, kterým byla uznána nemoc z povolání. Tyto osobní údaje se zpracovávají po dobu trvání pracovního poměru a dále pak v souladu s právními předpisy týkajícími pracovních úrazů a nemocí z povolání. Následně se likvidují.

Osobní údaje subjektu údajů, které jsou ve zmiňovaných databázích, jsou obsaženy na formulářích, ve smlouvách a dalších dokumentech, jenž jsou uchovávány v uzamykatelných skříních, v uzamykatelných prostorách společnosti, ke kterým má přístup pouze vymezený okruh pověřených osob. Společnost činí vše pro to, aby byly shromažďovány dokumenty s minimálním rozsahem osobních údajů a dále pak aktuální údaje o subjektech údajů. Pokud dojde k aktualizaci osobních údajů, staré osobní údaje bezodkladně zlikviduje. Pravidla likvidace osobních údajů, resp. písemností, jsou stanoveny ve skartačním a archivačním řádu společnosti. Pověřené osoby, které pracují s osobními údaji, jsou povinny veškeré dokumenty obsahující osobní údaje ukládat do uzamykatelných skříní, a to vždy nejpozději na konci každého pracovního dne. Na konci každého pracovního dne pověřené osoby zkontrolují, zda jsou všechny uzamykatelné skříně uzamčeny a uzamknou před odchodem místnost. V průběhu dne jsou pověřené osoby povinny při opuštění místnosti, kde se dokumentace s osobními údaji nachází, tuto uzamknout. Prostory, ve kterých jsou uchovávány osobní údaje, neslouží k přijímání zaměstnanců společnosti a třetích osob/návštěv. Tyto se přijímají výhradně v zasedacích místnostech společnosti. Vstup do prostor budovy společnosti je pouze pro zaměstnance. Třetí osoby mohou vstoupit do budovy společnosti pouze po předchozí identifikaci na recepci společnosti.

Elektronická podoba osobních údajů v informačním systému společnosti, kde jsou evidovány získané osobní údaje a další informace důležité pro potřeby jejich dalšího zpracování. Údaje v této podobě jsou zpracovávány v jednotlivých databázích, prostřednictvím informačních systémů. Přístup do databází obsahujících osobní údaje mají pouze pověřeni zaměstnanci, dále osoby, které zabezpečují informační systémy společnosti pro zpracování osobních údajů a jiné osoby, které k tomu mají oprávnění na základě uzavřené smlouvy o zpracování osobních údajů (dále vše jako „pověřené osoby“). Přístup do informačních systémů společnosti je chráněn individuálním heslem pověřené osoby. Individuální heslo je vyžadováno zadat při každém přihlášení se. V případě, že pověřená osoba přeruší práci s databází a chce odejít od PC nebo práci

ukončí, je automaticky odhlášena. V případě ukončení smluvního vztahu pověřené osoby se společností je povinností správce sítě zajistit zrušení jeho účtu a hesla. Pro vnášení údajů do databázového programu je povoleno používat pouze počítačovou techniku ve vlastnictví společnosti. Přístup do počítačové techniky společnosti musí být chráněn heslem. Hesla do databázového programu a do počítačové techniky se aktualizují minimálně jednou za tři měsíce. Pověřené osoby zodpovědné za oblast informatiky u zaměstnavatele zabezpečují povinnosti společnosti při ochraně osobních údajů uložených na serverech, osobních počítačích, včetně přenosných tak, aby ochrana uložených dat byla zajištěna v souladu s aktuálními požadavky na počítačovou bezpečnost a v tomto stavu ji udržovat a dodržovat povinnost mlčenlivosti, tj. jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání. Pověřené osoby společnosti, zaměstnanci, pracující v personálním oddělení, tyto osoby mají přístup k databázím a zaměstnanci pracující v IT oddělení, kteří zabezpečují informační systém společnosti pro zpracování osobních údajů. Jedná se o osoby, které mají přístup do všech databází společnosti. Pověřené osoby jsou povinny zpracovávat osobní údaje subjektů údajů v souladu s touto směrnicí, osobně, tuto činnost nesmí přenechat jiné osobě ani využít pro takovou činnost třetí osoby. Porušení povinností zaměstnanců vyplývajících z ustanovení směrnice na nakládání s osobními údaji se považuje za závažné porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci a může být důvodem jednostranného ukončení pracovněprávního vztahu ze strany zaměstnavatele. S touto směrnicí musí být seznámeni všichni zaměstnanci, jakož i další osoby smluvně spolupracující se společností. Změny a dodatky k této směrnicí se vydávají písemnou formou. Revize směrnice je provedena v případě potřeby, zejména při změně příslušných právních předpisů. Ostatní práva a povinnosti neuvedené v této směrnicí se řídí Obecného nařízení (GDPR), a ustanoveními zákoníku práce.

Na základě zjištěných skutečností je možné říct, že společnost má jasně stanovená pravidla pro nakládání s osobními údaji. Všechny dotčené pracovníky, kterých se práce s osobními údaji týká, řádně s těmito pravidly seznámila a pravidla jsou dodržována. Směrnice je pravidelně revidována a na každou revizi je provedeno následné školení určených pracovníků.

Seznam použitých zdrojů

Literární zdroje

1. JANEČKOVÁ, E., BARTÍK, V., *Ochrana osobních údajů v pracovním právu*. Praha: Wolters Kluwer ČR, 2016, 192 s. ISBN 978-80-7552-145-3.
2. BRŮHA, D., BUKOVJAN, P., ČORNEJOVÁ H., KALVODA, A., LEŠTINSKÁ, V., PELECH, P., ROUČKOVÁ, D., SCHIED, Z., STÝBLO, J., ŠENK, Z., VALENTA, J., *Abeceda personalisty 2018*, 8. vyd. Praha: ANAG, 2018, 575 s. ISBN 978-80-7554-120-8.
3. BRŮHA, D., BUKOVJAN, P., ČORNEJOVÁ H., KALVODA, A., LEŠTINSKÁ, V., PELECH, P., ROUČKOVÁ, D., SCHIED, Z., STÝBLO, J., ŠENK, Z., TRYLČ, L., VALENTA, J., *Abeceda personalisty 2016*, 7. vyd. Praha: ANAG, 2016, 580 s. ISBN 978-80-7554-003-4.
4. ŽŮREK, J., *Praktický průvodce GDPR*, 1. dotisk. Praha: ANAG. 2017, 223 s. ISBN 978-80-7554-097-3.
5. BARTÍK, V., JANEČKOVÁ, E., *Ochrana osobních údajů v aplikační praxi (vybrané problémy)*. 4. vyd. Praha: Wolters Kluwer ČR, a.s., 2016, 304 s. ISBN 978-80-7552-141-5.
6. NAVRÁTIL, J., a kol., *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, 339 s. ISBN 978-80-7380-689-7.
7. BARTÍK, V., JANEČKOVÁ, E., *Zákon o ochraně osobních údajů s komentářem*. Praha: ANAG. 2010, 380 s. ISBN 978-80-7263-613-6.
8. POSPÍŠIL, I., LANGÁŠEK, T., ŠIMÍČEK, V., WAGNEROVÁ, E., a kol., *Listina základních práv a svoboda s komentářem*. Praha: Wolters Kluwer ČR, 2012, 931 s., ISBN 978-80-7357-750-6.
9. HLOUŠKOVÁ, P., HOFMANNOVÁ, E., KNEBL P., ROUČKOVÁ, D., SCHMIED, Z., SCHWEINER, P. TOMANDLOVÁ, L., *Zákoník práce prováděcí nařízení vláda a další související předpisy k 1. 2. 2018*. 11. aktualizované vydání. Praha: ANAG, 2018, 1295 s, ISBN 978-80-7554-115-4.
10. ŠUBRT, B., LEIBLOVÁ, Z., PŘÍHODOVÁ, V., SKOUMALOVÁ, A., DANĚK, A., PŘIKRYLOVÁ, H., KRAJČÍKOVÁ, Z., LUKEŠOVÁ, D., DORČÁKOVÁ, J., MIKYSKA, M., *Abeceda mzdové účetní 2018*. 28. aktualizované vydání. Praha: ANAG. 2018, 631 s, ISBN 978-80-7554-117-8.
11. KOUBEK, J., *Řízení lidských zdrojů*. 4. rozšířené a doplněné vydání. Praha: Management Press, 2007. 399 s. ISBN 978-80-7261-168-3

12. DUŠEK, J., *Metodika pro tvorbu bakalářských prací VŠERS*. České Budějovice: Vysoká škola evropských a regionálních studií. 2017. 66 s.

Elektronické zdroje

1. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. In *Povinně zveřejňované informace, GDPR, Právní předpisy, Předávání osobních údajů do zahraničí*[online]. Praha: UOOU. Dostupné z WWW: <<https://www.uoou.cz>>.

Legislativní dokumenty

1. ČESKO. Zákon č. 101 ze dne 25. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In *Sbírka zákonů České republiky*. 2000, částka 32, s. 1521 - 1532. Dostupné z WWW: <<http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2000&typeLaw=zakon&what=Rok&stranka=12>>.
2. ČESKO. Zákon č. 361 ze dne 31. 10. 2003 o služebním poměru příslušníků bezpečnostních sborů. In *Sbírka zákonů České republiky*. 2003, částka 121, s. 5850 - 5910. Dostupné z WWW: <<http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2003&typeLaw=zakon&what=Rok&stranka=4>>.
3. ČESKO. Zákon č. 435 ze dne 23. 7. 2004 o zaměstnanosti. In *Sbírka zákonů České republiky*. 2004, částka 143, s. 8270 - 8316. Dostupné z WWW: <<http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2004&typeLaw=zakon&what=Rok&stranka=10>>.
4. ČESKO. Zákon č. 89 ze dne 22. 3. 2012 občanský zákoník. In *Sbírka zákonů České republiky*. 2012, částka 33, s. 1026 - 1367. Dostupné z WWW: <<http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2012&typeLaw=zakon&what=Rok&stranka=16>>.
5. ČESKO. Vyhláška č. 645 ze dne 22. 12. 2004, kterou se provádí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů. In *Sbírka zákonů České republiky*. 2004, částka 220, s. 11637 - 11663. Dostupné z WWW: <<http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2004&typeLaw=zakon&what=Rok&stranka=2>>.

Články

1. LIŠKUTÍN, T. Ochrana soukromí a osobních údajů zaměstnanců (GDPR). *Praktická personalistika*. 2018. č. 1-2, s. 7. ISSN2336-5072
2. LIŠKUTÍN, T. Ochrana soukromí a osobních údajů zaměstnanců (GDPR) – I. část. *Praktická personalistika*. 2018. č. 3-4, s. 7. ISSN2336-5072

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- Databáze řízení dokumentace společnosti,
- Kodex chování

Seznam zkratk

GDPR	General Data Protection Regulation, česky nařízení Evropského parlamentu a Rady (EU), obecné nařízení o ochraně osobních údajů
GPS	Global Positioning System, česky Globální polohový systém
HR	Human Resorsess, český personální oddělení
IT	Informační technologie
MNG	Management (vedení společnosti)
POP	Pomocně obslužný personál
THP	Technicko-hospodářský pracovník
ÚOOÚ	Úřad pro ochranu osobních údajů
VYRD	Výrobní dělník

Seznam obrázků

Obrázek č. 1: Informace o společnosti

Obrázek č. 2: Organizační členění společnosti

Obrázek č. 3: Produkty společnosti

Seznam grafů

Graf č. 1: Složení společnosti dle kategorie pracovníků

Graf č. 2: Pracovní pozice účastníků ověřování

Graf č. 3: Otázka č. 1: Jak dlouho pracujete ve společnosti?

Graf č. 4: Otázka č. 2: Znáte doporučení GDPR?

Graf č. 5: Otázka č. 3: Má společnost zpracovanou celofiremní směrnici o ochraně osobních údajů?

Graf č. 6: Otázka č. 4: Používá společnost k monitorování služebních vozů systém GPS?

Graf č. 7: Otázka č. 5: Jste si vědom, že v průběhu trvání pracovního poměru poskytnete svému zaměstnavateli své osobní údaje?

Graf č. 8: Otázka č. 6: Vyžaduje Váš zaměstnavatel souhlas s uveřejněním Vaší fotografie ve firemním časopise?

Graf č. 9: Otázka č. 7: Informoval Vás zaměstnavatel, že můžete kdykoliv souhlas s poskytováním osobních údajů odvolat?

Graf č. 10: Otázka č. 8: Zeptal se Vás nadřízený na zvláštní kategorii osobních údajů?

Graf č. 11: Otázka č. 9: Rozlišujete kategorie osob, u kterých zpracováváte osobní údaje?

Graf č. 12: Otázka č. 10: Informoval Vás zaměstnavatel, že předává Vaše osobní údaje do zahraničí?