ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

Katedra pracovního práva a práva sociálního zabezpečení

DIPLOMOVÁ PRÁCE

Ochrana osobních údajů v pracovněprávních vztazích

Markéta Kulichová

Plzeň 2020

Prohlášení

„*Prohlašuji, že jsem tuto diplomovou práci zpracovala samostatně a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala způsobem ve vědecké práci obvyklým.*“

V Plzni, duben 2020 _____

Markéta Kulichová

Poděkování

Ráda bych tímto poděkovala vedoucímu mé diplomové práce Mgr. Miroslavu Hromadovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při jejím vedení.

Obsah

Seznam použitých zkratek

ČR	Česká republika
EU	Evropská unie
ESLP	Evropský soud pro lidská práva
GDPR	nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
Listina	usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod
OSN	Organizace spojených národů
Sbor	Evropský sbor pro ochranu osobních údajů
Směrnice 95/46/ES	směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
SDEU	Soudní dvůr Evropské unie
ÚOOÚ	Úřad pro ochranu osobních údajů
WP 29	Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená směrnicí 95/46/ES podle článku 29
ZOOÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
ZZOÚ	zákon č. 110/2019 Sb., o zpracování osobních údajů

Úvod

Ochrana osobních údajů je v současné době aktuálním a diskutovaným tématem. Opětovné pozornosti se tomuto tématu dostalo především díky ne příliš dlouho účinnému nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, známému také pod názvem GDPR (General Data Protection Regulation) či Obecné nařízení. Přijetí tohoto nařízení není ničím jiným než reakcí na neustále se vyvíjející společnost a potřebu na tento fakt reagovat také v oblasti práva. Žijeme v období, kdy je svět digitalizován a pokrok technologií jde neustále vpřed. Tohoto jevu si je vědom i Ústavní soud ČR, který ve svém nedávno publikovaném nálezu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17-1 konstatuje, že *„dosah internetu a dalších sítí umožňujících elektronickou komunikaci se neomezují na hranice jednotlivých států, jde o globální jev, celosvětový fenomén, který vnitrostátní zákonodárci řeší různě a obtížně.“* S tím se pojí i různá rizika, a proto je nutné věnovat zvýšenou pozornost ochraně osobních údajů.

K výběru tohoto tématu mě inspirovalo setkání se s problematikou ochrany osobních údajů v pracovněprávních vztazích a obecně s pracovním právem jako takovým v praxi. S pracovním procesem se za svůj život setká každý z nás, ať již z pozice zaměstnance, či zaměstnavatele. Z toho důvodu považuji problematiku ochrany osobních údajů za něco, s čím by měl být každý alespoň v základní podobě obeznámen. Osobní údaj vnímám jako komoditu, kterou by si každý jedinec měl chránit. Avšak v praxi se můžeme setkat s tím, že leckdo bere toto téma na lehkou váhu. Ku příkladu v poslední době se rozmohl trend sociálních sítích, respektive sdílení soukromého života na sociálních sítích, což „nahrává do karet“ případným zaměstnavatelům, kteří si tak mohou poměrně rychle vyhledat informace o uchazečích a již na základě těchto vyhledaných údajů mají možnost se rozhodnout, zda vůbec uchazeče pozvou na pohovor. Lidé si tak mnohdy neuvědomují, jaké následky mohou mít jejich jednání, jak hájit svá práva a jaká práva obecně jim jako subjektům údajů náleží.

Jsem si vědoma toho, že téma diplomové práce je široké a lze na něj pohlížet z několika úhlů. Vzhledem k obsáhlosti tématu není mým cílem obsáhnout všechny

aspekty týkající se ochrany osobních údajů, nýbrž seznámit čtenáře s problematikou ochrany osobních údajů v pracovněprávních vztazích, podat přehled základních pojmů a právní úpravy, informovat je o zpracování osobních údajů v jednotlivých fázích pracovního poměru a dále nastínit vybrané instituty sledování zaměstnanců. Vše se zaměřením jak na práva a oprávněné zájmy zaměstnavatele, tak i práva zaměstnanců na soukromí jako takové.

Diplomová práce je založena především na analýze právní úpravy a judikatury v souvislosti s kompilací odborných děl. Práce je vnitřně členěna na čtyři na sebe navazující kapitoly. První kapitola je zaměřena na vymezení základních pojmů, která je dále rozvětvena na dvě části, a to na právní úpravu orientující se na pracovněprávní vztahy a základní terminologii, která doprovází celou práci. V druhé kapitole se zabývám vybranými povinnostmi zaměstnavatele a právy zaměstnance. Kapitola třetí je zacílena na zpracování osobních údajů v jednotlivých fázích pracovního poměru. Poslední kapitola by teoreticky mohla být součástí kapitoly třetí, avšak pro lepší přehlednost jsem se rozhodla ji vyčlenit, orientuje se na problematiku sledování zaměstnanců.

Je nutné si hned na samém počátku vytyčit pojem pracovněprávní vztah, kterým je v této práci myšlen pouze pracovní poměr.

Tato diplomová práce vychází z právního stavu účinného ke dni 9. 4. 2020.

1 Vymezení základních pojmů

Ačkoliv se v této práci hodlám zabývat spíše praktickými otázkami, nelze tak učinit bez objasnění základních pojmů pro lepší orientaci v dané oblasti. Z toho důvodu se v této kapitole věnuji právní úpravě ochrany osobních údajů s důrazem na právní úpravu související s pracovněprávními vztahy a dále se zabývám základní terminologií.

1.1 Právní úprava

Když se řekne „ochrana osobních údajů“, jistě každému, zejména pak laické veřejnosti, hned na mysl vyvstane GDPR. Není se čemu divit, neboť média opakovaně veřejnost utvrzovala v tom, že se jedná o předpis revoluční. Toto nařízení však není jedinou regulací, která dopadá na oblast pracovněprávních vztahů. Předmětem této práce není podat vyčerpávající přehled všech právních úprav platných v minulosti či současnosti, které se jakýmkoliv způsobem dotýkají ochrany osobních údajů. Pro účely práce je však nezbytné nastolit alespoň ve stručnosti právní úpravu, a to na úrovni mezinárodní, unijní i národní.

1.1.1 Mezinárodní právní úprava

S ohledem na časovou posloupnost vývoje ochrany osobních údajů je na místě prvně zmínit mezinárodní právní úpravu. Za základ práva na ochranu osobních údajů a práva na soukromí vůbec je považována Všeobecná deklarace lidských práv přijatá Valným shromážděním Organizace spojených národů roku 1948. Tento klíčový, avšak nezávazný, dokument v čl. 12 stanovoval také zákaz svévolného zasahování do soukromého života a korespondence. Všeobecná deklarace lidských práv připravila živnou půdu pro již právně závazný Mezinárodní pakt o občanských a politických právech přijatý Valným shromážděním OSN roku 1966, který se ochraně osobních údajů věnoval v čl. 17 a v podstatě přejímá obsah čl. 12 Všeobecné deklarace lidských práv.

V návaznosti na Všeobecnou deklarace lidských práv v roce 1950 byla Radou Evropy přijata Úmluva o ochraně lidských práv a základních svobod, též označována jako Evropská úmluva o lidských právech. Nicméně i Evropská úmluva o lidských právech se dotýká ochrany osobních údajů jen okrajově. Pro oblast práva ochrany osobních údajů je stěžejní čl. 8 týkající se práva na respektování rodinného

a soukromého života.[1] Tímto článkem je rovněž garantováno nezasahování do těchto práv ze strany státních orgánů. Článek se však nevypořádává s následky možného zásahu do těchto práv soukromou osobou.[2]

Významným dokumentem se stala až Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat z roku 1981, známá také pod názvem Úmluva č. 108. Tento mezinárodní dokument se od předchozích mezinárodních dokumentů lišil svojí konkrétností i závazností. V současné době Úmluvu č. 108 ratifikovalo 53 států. V ČR Úmluva vstoupila v platnost ke dni 1. listopadu 2001, tedy až po nabytí účinnosti zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.[3] Úmluva č. 108 obsahuje definice základních pojmů[4], přičemž pojem „osobní údaj", „správce" a „zpracování" se co do významu nikterak neliší od současného pojetí těchto pojmů. Úmluva také klade důraz ve svém čl. 6 na zvláštní skupinu údajů, tj. osobní údaje týkající se rasy, politických názorů, náboženského přesvědčení, zdraví, pohlavního života a odsouzení za trestný čin osoby. Působnost Úmluvy je stanovena na automatizované soubory a osobní údaje a jejich zpracování jak ve veřejném sektoru, tak i v sektoru soukromém.[5]

1.1.2 Unijní právní úprava

Evropská unie je založena na volném pohybu osob, zboží a služeb, s čímž souvisí i pohyb osobních údajů.[6] V rámci primárního práva EU je stěžejním pro ochranu osobních údajů čl. 16 Smlouvy o fungování Evropské unie zaručující právo každého na ochranu osobních údajů, které se ho týkají. Nelze opomenout ani Chartu základních práv EU, která se původně jako nezávazná politická deklarace po ratifikaci Lisabonské smlouvy stala součástí primárního práva EU[7] a ve svém čl. 8 odst. 1 deklaruje právo každého člověka na ochranu údajů osobního

[1] Čl. 7 odst. 1 Evropské úmluvy o lidských právech „Každý má právo na respektování svého soukromého života, obydlí a korespondence.
[2] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. ISBN 978-80-7502-275-2, s. 41.
[3] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 58-59.
[4] Srov. Čl. 2 Úmluvy č. 108 – osobní údaj, automatizovaný soubor dat, automatizované zpracování, správce souboru údajů
[5] Čl. 3 Úmluvy č. 108.
[6] Recitál 3 Směrnice 95/46/ES.
[7] Euroskop. Listina základních práv EU. *Euroskop.cz* [online]. Vláda České republiky [cit. 10. 2. 2020]. Dostupné z: https://www.euroskop.cz/204/sekce/charta-zakladnich-prav-eu/

charakteru. V následujícím odst. 2 téhož článku se promítají některé zásady nakládání s osobními údaji. Čl. 8 odst. 3 pak zakotvuje možnost kontroly dodržování zmíněných pravidel nezávislou mocí.

Postupem času se pod vlivem neustálého vývoje společnosti a moderní technologie svět začal globalizovat. Docházelo například ve větší míře k předávání osobních údajů i do třetích zemí. S tímto faktem se Evropská unie musela nějak vypořádat. Vnitrostátní úpravy států v tomto ohledu nebyly dostačující, a proto nastala nutnost rámcově sjednotit pravidla pro zacházení s osobními údaji. Sjednocujícím instrumentem se tak stala směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Ustanovení Úmluvy č. 108 se promítla ve směrnici 95/46/ES, avšak směrnice na rozdíl od Úmluvy se s úpravou ochrany osobních údajů vypořádala komplexněji. Směrnice 95/46/ES se vztahovala na částečně i plně automatizované zpracování a nově i na neautomatizované zpracování osobních údajů. Členským státům EU tak vzhledem k přijetí směrnice 95/46/ES vyvstala povinnost přijmout do svých právních řádů právní předpis, který by naplňoval cíl směrnice 95/46/ES. Účel směrnice 95/46/ES je obsažen v úvodních recitálech a jedná se zejména o ochranu osobních údajů v souvislosti se zpracováním osobních údajů a volný pohyb osobních údajů jakožto součást již zmíněného pohybu zboží, služeb, kapitálu a pracovních sil. ČR účel směrnice 95/46/ES naplnila skrze euronovelu ZOOÚ.[8]

Čl. 28 směrnice 95/46/ES stanovil členským státům povinnost ustanovit orgán dozoru, který by na svém území vykonával dohled nad dodržováním předpisů. V ČR se takovým orgánem stal Úřad pro ochranu osobních údajů, který byl zřízen dle § 2 ZOOÚ, přičemž jako ústřední správní úřad pro oblast ochrany osobních údajů byl považován až od 1. 1. 2015, tj. od účinnosti zákona č. 250/2014 Sb., o změně zákonů souvisejících s přijetím zákona o státní službě.

Významnou roli v oblasti ochrany osobních údajů sehrála Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, známá též pod označením WP 29 („Working party“) zřízená čl. 29 směrnice 95/46/ES.

[8] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 69 a 73.

WP 29 byl nezávislý poradní orgán Evropské komise, který plnil poradní funkci a mezi jeho činnosti patřilo zejména posuzování uplatňování vnitrostátních předpisů, zaujímání stanovisek či poskytování poradenství Evropské komisi. Mezi další úkoly patřila i povinnost oznámit Evropské komisi rozpory právních úprav členských států s jejich praxí, pokud by tak mohla být narušena rovnost ochrany osob v souvislosti se zpracováním osobních údajů v rámci EU.[9]

EU se tak podařilo díky směrnici 95/46/ES sjednotit alespoň základní rámec úpravy ochrany osobních údajů, nicméně právní úpravy jednotlivých členských států se postupem času v některých otázkách začaly od sebe výrazněji lišit.[10] Od doby přijetí směrnice 95/46/ES se rozvoj nových technologií opět posunul o něco dál a prostředky ke zpracování osobních údajů jsou dnes rozsáhlejší, než tomu bylo před pár lety. Vzhledem k tomuto stavu přestala směrnice 95/46/ES vyhovovat současné době a EU byla nucena podniknout další kroky směřující ke kýženému souladu právních úprav členských států a k poskytnutí fyzickým osobám větší ochrany jejich osobním údajům.

Tímto krokem bylo přijato Obecné nařízení, coby generální právní předpis pro oblast osobních údajů, které svou formou přímo a bezprostředně zavazuje členské státy bez nutnosti provádění dalších vnitrostátních opatření k učinění závaznosti právní normy. GDPR ve svém recitálu 9 zmiňuje, že jsou v úpravě převzaty cíle a zásady směrnice 95/46/ES a dále poukazuje na riziko rozdílnosti národních úprav ochrany osobních údajů členských států vyplývající z rozdílu v provádění směrnice 95/46/ES. Účelem GDPR je nesporně nastolení jednotné úpravy ochrany fyzických osob, a tím tak poskytnutí právní jistoty a transparentnosti.[11]

Jak již bylo uvedeno, GDPR byl ze strany médií označován jako předpis revoluční. Avšak po bližším zkoumání obsahu GDPR nikterak základní strukturu zpracování osobních údajů nemění, pouze dosavadní instituty zpřesňuje či pozměňuje. V čl. 68 GDPR dochází k nahrazení WP 29 nově zřízeným Evropským sborem pro ochranu osobních údajů. Sbor oproti WP 29 disponuje především rozšířenými pravomocemi, kdy může například rozhodovat spory mezi dozorovými

[9] Čl. 30 Směrnice 95/46/ES.
[10] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN: 978-80-7554-152-9, s. 15.
[11] Recitál 13 GDPR.

úřady či rozhodovat o postupech v naléhavých případech. Další oprávnění Sboru jsou uvedena v čl. 70 GDPR, zejména pak poskytování poradenství Evropské komisi či publikace výkladových dokumentů. Rozdíl mezi WP 29 a Sborem je také dán v právní subjektivitě, kdy Sboru, na rozdíl od WP 29, je právní subjektivita přiznána.[12] GDPR přichází také s novými povinnostmi pro správce, jako je např. informační povinnost vůči subjektu údajů, povinnost správců vést záznamy o činnostech zpracování či ohlašování případů porušení zabezpečení osobních údajů dozorovému orgánu. Subjekt údajů se může těšit z rozšíření katalogu práv, zejména právo na přenositelnost osobních údajů. Subjekt údajů má tak větší kontrolu nad zpracováním osobních údajů, které se týkají jeho osoby.

1.1.3 Národní právní úprava

Mezi právní předpis nejvyšší právní síly, co se týče ochrany osobních údajů, patří v ČR nepochybně Listina základních práv a svobod, která byla vyhlášena jako součást ústavního pořádku ČR usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. Konkrétně se jedná o čl. 7 odst. 1, který garantuje nedotknutelnost osoby a jejího soukromí, čl. 10 týkající se práva na zachování lidské důstojnosti, osobní cti, dobré pověsti a jména[13] a čl. 13[14] zaručující listovní tajemství. Z toho vychází fakt, že právo na ochranu osobních údajů je neoddělitelně spjato s právem na ochranu soukromí. Listina tedy vzhledem k právní síle vytváří základní právní rámec pro uplatňování práva na ochranu osobních údajů. Na Listinu a ochranu osobních údajů s ní spjatou navazují další předpisy nižší právní síly. Existuje celá řada právních předpisů souvisejících s ochranou osobních údajů.

Pracovněprávní vztahy se řídí zákoníkem práce[15] a ochrana osobních práv zaměstnance je zmíněna v § 316. Dále pak § 30 odst. 2 zákoníku práce se věnuje

[12] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, KOVAŘÍKOVÁ, Kristýna. *GDPR. Obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR, 2018. ISBN 978-80-7598-068-7, s. 485.
[13] Čl. 10 *Listiny základních práv a svobod „(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.“*
[14] Čl. 13 *Listiny základních práv a svobod „Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů, které stanoví zákon. Stejně se zaručuje tajemství zpráv podaných telefonem, telegrafem nebo jiným podobným zařízením.“*
[15] § 4 zákoníku práce.

právu zaměstnavatele získávat osobní údaje od uchazeče o zaměstnání, zejména pak omezení tohoto práva, neboť zaměstnavatel smí požadovat od uchazeče o zaměstnání pouze ty údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy. Úzké propojení s tímto ustanovením lze shledat v § 12 zákona č. 435/2004 Sb., o zaměstnanosti, který řeší zákaz vyžadování konkrétních informací od uchazečů o zaměstnání. Dále je třeba upozornit na § 312 zákoníku práce, který upravuje vedení osobního spisu obsahujícího osobní údaje zaměstnance. Ještě zmíním § 4 zákoníku práce, neboť toto ustanovení upravuje mimo jiné i vzájemný vztah zákoníku práce a zákona č. 89/2012 Sb., občanského zákoníku.

Zákoník práce je svou povahou právním předpisem zvláštním a občanský zákoník právním předpisem obecným. Vztah mezi těmito předpisy je založen na zásadě subsidiarity, kdy se na pracovněprávní vztahy použijí ustanovení občanského zákoníku v případě, že zákoník práce sám určité otázky neupravuje.[16] Otázky ochrany soukromí jsou upraveny v § 81 an. občanského zákoníku. Za zmínku stojí i § 2956 občanského zákoníku, podle kterého se lze domoci náhrady škody i nemajetkové újmy způsobené zásahem do soukromí. Ochranu poskytuje také zákon č. 40/2009 Sb., trestní zákoník, který obsahuje ve své zvláštní části, přesněji v § 180 an., trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství.[17]

První komplexnější právní úpravou pro oblast ochrany osobních údajů se stal až zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. ZOOÚ byl několikrát novelizován. Jak již bylo uvedeno, významnou novelizací prošel v roce 2004 v souvislosti se vstupem ČR do EU, a tím i nutností naplnění účelu směrnice 95/46/ES.

Ke dni účinnosti GDPR, tj. 25. května 2018, měl být ZOOÚ zrušen a na místo něho přijat adaptační zákon, který zejména připraví právní řád ČR na dopad GDPR.[18] To se však nestalo a v českém právním řádu tak nastal nežádoucí stav,

[16] Nález Ústavního soudu ČR publikován pod č. 116/2008 Sb., ze dne 12. 3. 2008 ve věci návrhu na zrušení některých ustanovení zákona č. 262/2006 Sb., zákoník práce.
[17] Jedná se o trestný čin (dále jen „TČ“) neoprávněné nakládání s osobními údaji (§ 180), TČ poškození cizích práv (§ 181), TČ porušení tajemství dopravovaných zpráv (§ 182) a TČ pomluvy (§ 184).
[18] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN: 978-80-7554-152-9, s. 19.

kdy bylo účinné GDPR, zároveň byl nadále také účinný ZOOÚ a předvídaný adaptační zákon přijat nebyl. Tento nesoulad bylo dle mého názoru možné shledat zejména v narušení právní jistoty adresátů právních norem. ZOOÚ a další vnitrostátní právní předpisy upravující oblast ochrany osobních údajů mohly být aplikovány pouze v souladu s GDPR. V případě rozporu se situace řeší použitím základní zásady práva EU – zásadou aplikační přednosti práva EU, která stanoví, že v případě aplikační kolize mezi přímo použitelnou normou práva EU s vnitrostátní normou má aplikační přednost norma práva EU.[19]

Nesouladný stav v právním řádu ČR trval až do 24. 4. 2019, tedy do účinnosti zákona č. 110/2019 Sb., o zpracování údajů. ZZOÚ zastává roli doplňkového zákona k GDPR, nejedná se o svébytný zákon. Jeho účelem není kopírovat obsah GDPR, jako je tomu tak u našeho sousedního státu – Slovenska, kde byl přijat zákon č. 19/2018 Z.z., o ochrane osobných údajov. Cílem ZZOÚ je zejména provedení implementace GDPR a zajištění adaptace na toto nařízení.[20] Krom toho tento zákon zastává ještě další roli, a to roli transpozičního zákona, kterým se provádí směrnice Evropského parlamentu a Rady (EU) 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestních činů nebo výkonu trestu. Tyto dvě skutečnosti, resp. dvě role tohoto zákona, se odráží v systematice ZZOÚ.[21] ZZOÚ ve vztahu ke zpracování osobních údajů dle GDPR upravuje ty otázky, u kterých GDPR předpokládá, že se jimi členské státy budou samy prostřednictvím vnitrostátních právních předpisů zabývat.[22] Mezi tyto otázky patří například určení věku dítěte pro udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti.

Členské státy mají možnost právním předpisem nebo kolektivními smlouvami zavést konkrétnější pravidla k zajištění ochrany práv a svobod v oblasti zpracování osobních údajů zaměstnanců.[23] Přijetím ZZOÚ však nedošlo k žádnému zavedení takových pravidel.[24]

[19] Rozsudek ESD ze dne 15. 7. 1964, Flaminio Costa proti E.N.E.L., věc C-6/64, EU:C:1964:66.
[20] 138/0 vládní návrh na vydání zákona o zpracování osobních údajů.
[21] ŽŮREK, Jiří. *K zákonu o zpracování osobních údajů*. Praktická personalistika, č. 5-6/2019, s. 12-14.
[22] Srov. Recitál 8 GDPR.
[23] Čl. 88 GDPR.
[24] 138/0 vládní návrh na vydání zákona o zpracování osobních údajů.

1.2 Základní terminologie ochrany osobních údajů

Pro účely této diplomové práce je zapotřebí si vymezit základní terminologii, se kterou budu v průběhu práce pracovat. Co se týče vnitrostátní právní úpravy osobních údajů – ZZOÚ neobsahuje vlastní definice pojmů, takže v této podkapitole vychází vymezení pojmů zejména z GDPR z aktuálního znění. Nejde zde však o vyčerpávající výčet pojmů, ale jedná se o nastolení pojmů, které považuji za nezbytné v souvislosti s pracovněprávním vztahem a případné další pojmy budou vysvětleny v průběhu práce. Co se týče předchozích již zrušených právních úprav ochrany osobních údajů – směrnice 95/46/ES a ZOOÚ, je zde na místě podotknout, že s účinností GDPR nedošlo k zásadním změnám definic a obecně interpretace uvedených pojmů.

1.2.1 Osobní údaj

Pojem osobní údaj je vesměs klíčovým pojmem celé problematiky ochrany osobních údajů. Osobní údaj je v čl. 4 odst. 1 GDPR vymezen jako jakákoli informace o identifikované nebo identifikovatelné fyzické osobě. Tuto fyzickou osobu lze přímo nebo nepřímo identifikovat pomocí určitých identifikátorů. Fyzickou osobou se v případě pracovního poměru myslí uchazeč, zaměstnanec nebo bývalý zaměstnanec, který stojí v právním vztahu proti zaměstnavateli – správci osobních údajů. Pokud daný údaj nespadá pod tuto definici, nelze ho považovat dle GDPR za osobní údaj a takový údaj není tudíž chráněn GDPR. GDPR rovněž neposkytuje ochranu právnickým osobám.[25]

Za osobní údaje jsou jednak považovány ty identifikační údaje, díky nimž lze jasně identifikovat konkrétní osobu, například jméno, příjmení, rodné číslo či adresa, jednak všechny informace, které v konečné sestavě dávají o dané osobě ucelený obraz, avšak samostatně tyto informace nejsou schopné osobu jednoznačně identifikovat, jako například dosažené vzdělání, mzda.[26] Jinými slovy pod pojem osobní údaj, lze řadit i údaj, který na „první pohled“ nemusí vůbec jako osobní údaj vypadat. Jsou-li konkrétní informace spojitelné s jinými dalšími informacemi a na základě toho lze identifikovat osobu, bude se v takovém případě jednat o osobní

[25] Recitál 14 GDPR.
[26] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, KOVAŘÍKOVÁ, Kristýna. *GDPR. Obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR, 2018. ISBN 978-80-7598-068-7, s. 77-78.

údaj. Na osobní údaj tedy nelze nahlížet separovaně, neboť za osobní údaj se považují jak údaje identifikační, tak i další údaje, které se týkají dané osoby v okamžiku, kdy se stane dostatečně identifikovanou či je identifikovatelná.[27] „*Při určování, zda je fyzická osoba identifikovatelná, by se mělo přihlédnout ke všem prostředkům, jako je například výběr vyčleněním, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou nebo nepřímou identifikaci dané fyzické osoby.*“[28]

Občanský zákoník v § 3019 uvádí výčet údajů, na jejichž základě je možné identifikovat osobu fyzickou. Těmito údaji jsou zejména jméno, bydliště a datum narození. Jedná se o demonstrativní výčet údajů, avšak tyto tři údaje jsou ve svém souhrnu schopné zajistit ztotožnění fyzické osoby. *„Za osobní údaj však zdejší soud nepovažuje ani jméno a příjmení osoby (návštěvníka) ve spojení s číslem jeho občanského průkazu. Ani na základě těchto údajů totiž není možné konkrétní osobu určit nebo kontaktovat. Neexistuje totiž žádný veřejně dostupný registr čísel občanských průkazů, v němž by bylo možné zjistit identitu osoby podle čísla průkazu. Navíc v případě čísla občanského průkazu se jedná o označení, které je v průběhu času proměnlivé. Fyzická osoba totiž neobdrží jedno číslo občanského průkazu na celý život, nýbrž při každé výměně tohoto průkazu získává průkaz s číslem novým.“* [29] S názorem ohledně čísla občanského průkazu vyřčeným Nejvyšším správním soudem se ztotožňuji.

Ačkoliv byla WP29 účinností GDPR nahrazena Evropským sborem pro ochranu osobních údajů, lze stanoviska WP29 i nadále použít, neboť výklad pojmu osobního údaje se nikterak neliší od definice tohoto pojmu z předchozích právních úprav – směrnice 95/46/ES a ZOOÚ. Mezi významnou interpretační pomůcku patří stanovisko č. 4/2007 WP29 k pojmu osobní údaje, které mimo jiné obsahuje i praktické příklady. Zmíněné stanovisko dělí informace vztahující se k osobnímu údaji na objektivní (např. přítomnost určité látky v krvi) a subjektivní (např. názory, hodnocení). Forma těchto informací je různorodá, mohou mít podobu textovou, číselnou, grafickou, fotografickou či zvukovou. Aby byl vůbec nějaký údaj považován za osobní údaj, nemusí být pravdivý či ověřený. V takovém případě má subjekt údajů dle GDPR právo na opravu, výmaz nebo omezení zpracování.

[27] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 21.
[28] Recitál 26 GDPR.
[29] Rozsudek Nejvyššího správního soudu ze dne 29. 7. 2009, sp. zn. 1 As 98/2008-148.

GDPR v čl. 4 odst. 1 mezi identifikátory nově zařazuje lokační a síťové identifikátory, což lze vnímat jako posílení právní jistoty správce osobních údajů, neboť v předchozí právní úpravě – směrnici 95/46/ES a ZOOÚ se v definicích pojmu osobního údaje zmíněné identifikátory nevyskytovaly. Tento fakt je však třeba vnímat pouze jako rozšíření demonstrativního výčtu, nikoli rozšíření samotné definice pojmu. U pojmu osobních údajů se nelze uchýlit k taxativnímu výčtu z důvodu samotné povahy osobního údaje. Osobní údaje nadále vznikají v souvislosti s rozvojem nových technologií ve společnosti, jako jsou například internetové technologie.[30] Lokalizačním údajem je údaj, který určuje polohu dané osoby – typicky např. využívání GPS ve služebních automobilech a následný údaj v knize jízd či funkce využívající údaje o poloze v mobilních telefonech. Otázku síťových identifikátorů řešil již před účinností GDPR i SDEU, přičemž v případě, kdy poskytovatel služeb disponuje právními prostředky, které jsou schopné identifikovat subjekt údajů na základě informací, jež má k dispozici poskytovatel internetového připojení daného subjektu údajů. V tomto případě jsou považovány za osobní údaje i síťové identifikátory, mezi něž patří i dynamická adresa IP.[31]

1.2.1.1 Pseudonymizované osobní údaje

Pseudonymizací se rozumí *„zpracování osobních údajů tak, že již nemohou být přiřazeny ke konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.“*[32] Předně je vhodné podotknout, že v pracovněprávních vztazích není pseudonymizace povinná. Subjektu údajů je přidělen jiný identifikátor (pseudonym), například osobní číslo, namísto běžného identifikátoru. V pracovněprávních vztazích je pak zaměstnanec na základě pseudonymu přímo identifikován pouze u zaměstnavatele a mimo něj přímo identifikován není. Pseudonymizace tak minimalizuje zásah do právem chráněných hodnot zaměstnanců.[33]

[30] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4, s. 277
[31] Rozsudek SDEU ze dne 19. 10. 2016, Patrick Breyer proti Spolkové republice Německo, věc C-582/14, EU:C:2016:779.
[32] Čl. 4 odst. 5 GDPR.
[33] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 26-27.

1.2.1.2 Zvláštní kategorie osobních údajů

V souvislosti s osobními údaji bych dále zmínila podkategorii osobních údajů, a to zvláštní kategorii osobních údajů. Zvláštní kategorie osobních údajů nahrazuje koncept citlivých údajů, avšak ve společnosti je již zažitý pojem „citlivý osobní údaj". Pojem „zvláštní kategorie osobních údajů" není zařazen mezi definice pojmů v čl. 4 GDPR, ale je mu věnován prostor v čl. 9 a 10 GDPR v oblasti zpracování zvláštních kategorií osobních údajů a dále se o této kategorii zmiňuje i recitál 10 a 51 GDPR. Je vhodné zmínit také fakt, že současné znění zákona č. 110/2019, o zpracování osobních údajů, se z důvodu právní jistoty věnuje v přechodném ustanovení v § 66 odst. 6 krátce pojmu citlivý údaj, resp. citlivý osobní údaj. Definice obsažená v tomto ustanovení odpovídá článkům 9 a 10 GDPR.[34] Zvláštní kategorii osobních údajů je nutné věnovat speciální pozornost, neboť tyto údaje jsou způsobilé přivodit subjektu údajů újmu,[35] například v případě znalosti takového osobního údaje může v zaměstnání dojít k diskriminaci zaměstnance jak ze strany zaměstnavatele, tak ze strany ostatních zaměstnanců.

„Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby."[36] Zde se oproti čl. 4 odst. 1 GDPR, který definuje již výše zmíněný osobní údaj, jedná o taxativní výčet, tudíž žádné další osobní údaje než tyto zmíněné v čl. 9 odst. 1 GDPR nejsou považovány za zvláštní kategorii citlivých údajů. Zákaz zpracování zvláštní kategorie osobních údajů je prolomen, pokud je zpracování nezbytné pro splnění právní povinnosti[37] vyplývající z právních předpisů, zejména zákoníku práce, předpisů o sociálním, nemocenském a zdravotním pojištění.

Z výše uvedeného výčtu údajů bych se ráda krátce věnovala genetickým údajům, biometrickým údajům a údajům o zdravotním stavu fyzické osoby, neboť s těmito druhy zvláštní kategorie osobních údajů se lze snadno setkat

[34] 138/0 vládní návrh na vydání zákona o zpracování osobních údajů.
[35] *Handbook on European data protection law* [online]. Luxembourg: Publications Office of the European Union, 2018, s. 96 [cit. 2019-11-23]. Dostupné z: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
[36] Čl. 9 odst. 1 GDPR.
[37] Čl. 6 odst. 1 písm. c) GDPR.

v pracovněprávních vztazích. Do zvláštní kategorie osobních údajů spadajících do kategorie genetických údajů řadíme zejména informace, které lze získat z analýzy biologických vzorků fyzické osoby, například výsledek z krevní zkoušky na alkohol. Za údaje související se zdravotním stavem lze považovat údaje týkající se fyzického nebo duševního zdraví fyzické osoby, například potvrzení o invaliditě zaměstnance[38] či údaj o tom, že si zaměstnanec poranil nohu, a z toho důvodu čerpá volno.[39] Potvrzení poskytovatele pracovnělékařských služeb o tom, že je uchazeč o zaměstnání zdravotně způsobilý k výkonu práce bez omezení naopak údajem o zdravotním stavu nebude. Dále do kategorie biometrických údajů patří například otisk prstu či dlaně, obraz oční sítnice či hlasový projev, například při monitorování pracovních telefonních hovorů. [40]

Dne 19. 3. 2020 přijal Sbor stanovisko ke zpracování osobních údajů v souvislosti s propuknutím nákazy COVID-19. Stanovisko řeší mimo jiné i zpracování citlivých údajů, přičemž poukazuje na GDPR, které předpokládá odchylky ze zákazu zpracování určitých kategorií osobních údajů. V souvislosti se zaměstnáním se jedná o zpracování zdravotních údajů, kdy je dle čl. 9 odst. 2 písm. i) GDPR zpracování nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví. Dále recitál 46 GDPR osvětluje, že některé druhy zpracování mohou sloužit pro humanitární účely, včetně monitorování epidemií a jejich šíření. Dle § 102 zákoníku práce vznikají zaměstnavateli určité povinnosti, a to především povinnost vytvářet bezpečné a zdraví neohrožující pracovní prostředí. V této situaci budou hrát roli zejména prevenční povinnosti, kdy zaměstnavatel je povinen postupovat tak, aby případná rizika byla minimalizována. V rámci preventivní povinnosti musí zaměstnavatelé informovat své zaměstnance o případných rizicích. Zaměstnavatel tak musí například informovat zaměstnance o tom, že na pracovišti se vyskytuje nebo vyskytovala nakažená osoba. Tyto informace zaměstnavatel poskytuje pouze v nezbytném rozsahu, vždy s ohledem na důstojnost dané osoby.[41]

---

[38] ŽUĽOVÁ, Jana, a kol. *Spracúvanie osobních údajov zamestnanca podľa GDPR (analýza GDPR na pracovisku).* Košice: Univerzita P. J. Šafárika v Košiciach, 2018. ISBN 978-80-8152-588-9, s. 14-16.

[39] Rozsudek SDEU ze dne 6. 11. 2003, Bodil Lindqvist proti Švédsku, věc C-101/01, EU:C:2003:596.

[40] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 128.

[41] Ke zpracování osobních údajů v rámci opatření proti šíření koronaviru: Poradna: Úřad pro ochranu osobních údajů. *Uoou.cz* [online]. [cit. 27. 3. 2020]. Dostupné z: https://www.uoou.cz/ke-zpracovani-osobnich-udaju-v-ramci-opatreni-proti-sireni-koronaviru/ds-6134/archiv=1&p1=2611

V poslední době se rozmohlo využívání systémů umožňujících určení fyzické osoby na základě biometrických znaků také v pracovněprávních vztazích. Jedná se tak například o využívání otisků prstů v přístupových a docházkových systémech. Vzhledem k přímému ztotožnění otisku s konkrétní osobou se má tak zamezit možnosti klamání zaměstnavatele. Pokud by zaměstnavatel však využíval evidenci takového údaje nad rámec evidence přítomnosti zaměstnance na pracovišti, mohl by se takovým jednáním dopustit porušení zákazu otevřeného i skrytého sledování zaměstnanců vyplývajícího z § 316 zákoníku práce.[42] Docházkové systémy tak na jednu stranu mohou zjednodušovat ověřování docházky zaměstnanců, ale na druhé straně mohou vést k nepřiměřeným zásahům do právem zaručených hodnot. Takové riziko lze minimalizovat pomocí pseudonymizace, jakožto techniky zabezpečení dle čl. 32 odst. 1 písm. a) GDPR.[43]

Mezi citlivé osobní údaje naopak nepatří fotografie, pokud fotografie není zpracovávána zvláštními technickými prostředky, které jsou schopné konkrétní fyzickou osobu jedinečně identifikovat nebo autentizovat.[44] Na opačné straně by pak bylo možné zachytit citlivou charakteristiku jako například rasu či zdravotní stav a šlo by tedy o zpracování citlivých osobních údajů. Citlivým osobním údajem není ani rodné číslo.[45] Podmínky využívání rodného čísla jsou stanoveny zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných čísel.

Citlivým osobním údajům věnuje pozornost i zákoník práce. V ustanovení § 316 odst. 4, jež stanovuje, které informace bezprostředně nesouvisejí s výkonem práce a pracovněprávním vztahem a které nesmí zaměstnavatel vyžadovat od zaměstnance. Výčet v tomto ustanovení však není úplný na rozdíl od výčtu osobních citlivých údajů uvedeném v GDPR. Zákoník práce naopak uvádí informace, které se ve výčtu v čl. 9 odst. 1 GDPR nenachází (viz kapitola 3.1). Je na místě zmínit problematiku rozdílného nahlížení na údaje vyplývající z výpisu trestního rejstříku. V praxi totiž dochází mnohdy k nakládání s výpisy

[42] Stanovisko ÚOOÚ č. 3/2009, revidované v červnu 2017 biometrická identifikace nebo autentizace zaměstnanců.
[43] MATES, Pavel (ed.), VALOUŠEK, Martin, FIALOVÁ, Eva, LECHNER, Tomáš, HÁLOVÁ, Markéta, SIVÁK, Jakub, SOVOVÁ, Olga, BRUNA, Eduard, BRUNOVÁ, Markéta. *Ochrana osobnosti, soukromí a osobních údajů.* Praha: Leges, 2019. ISBN 978-80-7502-346-9, s. 211.
[44] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 23.
[45] K rodným číslům: Úřad pro ochranu osobních údajů. *Uoou.cz* [online]. [cit. 24. 11. 2019]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5091&n=k%2Drodnym%2Dcislum

z rejstříků trestů ze strany zaměstnavatelů. Pokud výpis z trestního rejstříku obsahuje pozitivní informace o tom, že daná osoba byla pravomocně odsouzena, tak se na tyto informace pohlíží jako na citlivé osobní informace. V opačném případě, kdy výpis z trestního rejstříku neobsahuje žádné pozitivní informace, a jedná se tedy o důkaz o bezúhonnosti osoby, ale pouze to, že konkrétní fyzická osoba nemá záznam v trestním rejstříku, jedná se o „obyčejný" osobní údaj, nikoli citlivý osobní údaj. Citlivým osobním údajem nebude ani informace o tom, že trestní stíhání bylo zastaveno. [46]

Zaměstnavatel je povinen vést knihu úrazů, ve které se zaznamenávají všechny úrazy, a to i v případě, že nebyla způsobena pracovní neschopnost nebo byla způsobena pracovní neschopnost nepřesahující 3 kalendářní dny. [47] Zaměstnavatel je také povinen dle § 103 odst. 2 písm. c) zákoníku práce zajistit, aby některé činnosti vykonávali pouze zaměstnanci s platným zdravotním průkazem, kteří jsou očkováni nebo disponují dokladem o odolnosti vůči nákaze. V těchto případech se jedná o informaci o zdravotním stavu zaměstnance, což vyplývá z povahy takových údajů.

1.2.2 Subjekt údajů

Subjekt údajů je vymezen v GDPR v rámci pojmu osobních údajů jako identifikovaná nebo identifikovatelná fyzická osoba. Nejde přímo o definici tohoto pojmu, ale legislativní zkratku. ZZOÚ proto definuje subjekt údajů v § 3, a to jako fyzickou osobu, k níž se osobní údaje vztahují.[48] Subjektem údajů však nejsou zesnulé osoby.[49] V případě pracovněprávních vztahů je subjektem údajů zejména zaměstnanec, který je vůči zaměstnavateli (správci) v nerovném postavení. Toto nerovné postavení[50] mezi zaměstnancem a zaměstnavatelem je vyvažováno řadou oprávnění, která právními předpisy poskytují zaměstnanci (nejen) v oblasti ochranu osobních údajů (více kapitola 2). Jako další subjekty údajů přichází v úvahu také

[46] JANEČKOVÁ, Eva, BARTÍK, Václav. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 97 a 105-106.
[47] § 105 odst. 2 zákoníku práce.
[48] VLACHOVÁ, Barbora. *Zákon o zpracování osobních údajů: komentář*. V Praze: C.H. Beck, 2019. Beckovy komentáře. ISBN 978-80-7400-760-6, s. 7-8.
[49] Recitál 27 GDPR.
[50] § 2 odst. 1 zákoníku práce.

uchazeči o zaměstnání, dočasně přidělení zaměstnanci či rodinní příslušníci zaměstnance, pokud zaměstnavatel zpracovává jejich údaje.[51]

1.2.3 Správce, zpracovatel a příjemce

Vedle subjektu údajů jsou dalšími zásadními osobami v oblasti ochrany osobních údajů také správci a zpracovatelé. Správce je dle čl. 4 odst. 7 subjekt, který určuje účel a prostředky zpracování osobních údajů. Může tak jít o fyzickou osobu, právnickou osobu, orgán veřejné moci či agenturu. Správce se nachází v každém zpracování osobních údajů, kdežto zpracovatel je složkou fakultativní, neboť je na uvážení správce, zda do procesu zpracování zahrne i tento další subjekt.[52] Platí, že vždy za zpracování osobních údajů odpovídá správce, který má dále povinnost doložit, že činnosti zpracování jsou v souladu s GDPR.[53] [54]

Povinnost doložení, že činnosti zpracování jsou v souladu s GDPR, je jednou ze změn, kterou přineslo GDPR. Odpovědností správce se zabývá také čl. 24 GDPR, který tvrdí že: *„S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i různě pravděpodobným i různě závazným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být dle potřeby revidována a aktualizována*.“ Mezi další změny patří zavedení institutu společných správců v čl. 26 GDPR. Pokud pojem správce vztáhneme na pracovněprávní vztahy, bude se tak jednat o zaměstnavatele. Ten může zpracovávat osobní údaje skrze své zaměstnance.

Za předpokladu, že správce využije možnost proces zpracování osobních údajů převést na základě zpracovatelské smlouvy[55] na jiný subjekt (subjekt odlišný od správce), lze v takovém případě hovořit o zpracování osobních údajů zpracovatelem. Ten pak zpracovává osobní údaje pro správce[56] na základě jeho pokynů. Správce smí pověřovat pouze takové zpracovatele, kteří vykazují známky odbornosti, spolehlivosti a lze rozumně předpokládat, že jimi zavedená opatření

[51] ŽUĽOVÁ, Jana, a kol. *Spracúvanie osobních údajov zamestnanca podľa GDPR (analýza GDPR na pracovisku).* Košice: Univerzita P. J. Šafárika v Košiciach, 2018. ISBN 978-80-8152-588-9, s. 17.
[52] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN: 978-80-7554-152-9, s. 89-90.
[53] Čl. 5 odst. 2 GDPR.
[54] Recitál 74 GDPR.
[55] Čl. 28 GDPR.
[56] Čl. 4 odst. 8 GDPR.

budou splňovat požadavky GDPR. [57] Zpracovatel je veřejnoprávně i soukromoprávně odpovědný za zákonnost zpracování osobních údajů. V případě, že zpracování nebude v souladu s právními předpisy, může být zpracovatel odpovědný za přestupek či v soukromoprávní rovině za způsobenou hmotnou či nehmotnou újmu. [58] Pokud subjekt údajů (zaměstnanec) požaduje náhradu za utrpěnou újmu, musí prokázat, že újma vznikla v příčinné souvislosti s porušením GDPR ze strany zaměstnavatele.[59] Tento fakt však nemá žádný vliv na celkovou odpovědnost správce za zpracování osobních údajů. V pracovněprávních vztazích tak může jít o externí personalisty, externí mzdové účetní, IT poskytovatele služeb[60] apod. S ohledem na výše uvedené vyplývá, že za zpracovatele nejsou považováni zaměstnanci zaměstnavatele.

Příjemcem je dle čl. 4 odst. 9 GDPR jakákoli osoba odlišná od osoby správce či zpracovatele osobních údajů, jakožto i od osob, které vykonávají u správce nebo zpracovatele osobních údajů zpracovatelské činnosti. Za příjemce však nejsou považovány orgány veřejné moci, které mají k osobním údajům přístup v rámci výkonu své pravomoci.

1.2.4 Zpracování osobních údajů

Pojem zpracování osobních údajů patří mezi další klíčové pojmy, neboť obsah tohoto pojmu spolu s obsahem pojmu osobní údaj souvisí s vymezením věcné působnosti GDPR. Definice pojmu zpracování se nachází v čl. 4 odst. 2 GDPR a zpracováním se má na mysli „*jakékoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz či zničení.“* GDPR se nevztahuje na nakládání

[57] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-689-7, s. 79.
[58] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 156.
[59] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 174.
[60] V případě poskytování jednorázových služeb IT poskytovatelem služeb bez dalšího nakládání a zpracování s osobními daty nelze hovořit o IT poskytovateli jakožto o zpracovateli osobních údajů. Vždy je nutné pohlížet na souhrn činností, které poskytovatel IT služeb poskytuje. ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 167.

s osobními údaji jiným způsobem než zpracováním a dále se GDPR nevztahuje ani na zpracování informací, které nespadají pod definici osobního údaje.

Nahodilé shromažďování informací taktéž nepodléhá GDPR. Může tak jít například o nevyžádaný životopis, kdy uchazeč o zaměstnání zašle e-mailem potenciálnímu zaměstnavateli spolu s poptávkou práce svůj životopis bez vazby na konkrétní pracovní nabídku čistě „pro jistotu“. Pokud zaměstnavatel nebude nadále s údaji uvedenými v životopise nakládat a tento životopis zlikviduje, nebude se na takové jednání GDPR vztahovat. Pokud se však zaměstnavatel rozhodne údaje z životopisu zařadit do své evidence,[61] je v tomto případě nutné si pro tyto účely vyžádat souhlas se zpracováním osobních údajů daného uchazeče o zaměstnání. Za vyjádření souhlasu lze považovat mnohdy již samotné zaslání životopisu, pokud z uchazečova jednání vyplývá jeho vůle.[62]

Zpracováním osobních údajů se zabývá i nově účinný ZZOÚ, který ve své hlavě II stanovuje pravidla pro zpracování osobních údajů v režimu GDPR. Jsou zde zařazena ta zpracování, u kterých by mohla být pochybnost ohledně působnosti zákonné úpravy.

1.2.5 Souhlas se zpracováním osobních údajů

Souhlas subjektu údajů je specifikován v čl. 4 odst. 11 GDPR jako *„jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování osobních údajů.“* Nadále tak zůstává jako jeden z důvodů zákonného zpracování osobních údajů,[63] avšak oproti předešlé úpravě jsou v GDPR podmínky pro získávání souhlasu ke zpracování osobních údajů přísnější. Z výše uvedené definice vyplývá, že za souhlas nelze považovat mlčení.

Vzhledem k povaze pracovněprávních vztahů, tedy nerovného postavení mezi zaměstnavatelem a zaměstnancem, kdy zaměstnanec je zaměstnavateli podřízen a zaměstnanec v těchto právních vztazích vystupuje jako slabší strana, není využití souhlasu se zpracováním osobních údajů dost dobře možné. Souhlas

[61] Srov. čl. 4 odst. 6 GDPR pro účely tohoto nařízení se rozumí „evidencí“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.
[62] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 23-24 a 122.
[63] Srov. čl. 6 odst. 1 GDPR.

subjektu údajů nemůže být považován za svobodný, pokud nemá subjekt údajů skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout, aniž by mu neudělení souhlasu mohlo způsobit neblahé následky. Za takový následek může být považováno „v lepším případě“ například zhoršení mezilidských vztahů na pracovišti, v tom „horším případě“ například nepřiznání prémií.[64] Avšak výjimečně i v pracovněprávních vztazích mohou nastat případy, kdy zaměstnavatel bude schopen prokázat, že souhlas zaměstnance byl udělen skutečně svobodně. Z výše uvedeného plyne, že souhlas může být považován za skutečně svobodný pouze v případě, kdy neudělení takového souhlasu nebude mít pro zaměstnance nepříznivý účinek. [65] K nerovnováze v právním postavení a souhlasu se zpracováním osobních údajů v pracovněprávních vztazích se vyslovila i WP 29. „*Pro většinu zpracování dat na pracovišti nemůže a neměl by být právním důvodem souhlas zaměstnance vzhledem k povaze vztahu mezi zaměstnavatelem a zaměstnancem.“* Zaměstnavatelé se tak až na výjimečné situace musí opřít o jiný zákonný důvod než souhlas.[66]

Zákonným důvodem ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním je zejména plnění pracovní smlouvy,[67] plnění právní povinnosti [68] [69], neboť zpracování osobních údajů je nezbytné pro splnění povinností vycházejících z právních předpisů, zejména zákoníku práce, daňových předpisů, předpisů o sociálním, nemocenské a zdravotním pojištění nebo z přepisů upravujících bezpečnost ochrany zdraví při práci, anebo oprávněný zájem zaměstnavatele, který musí být blíže specifikován, tj. v čem oprávněný zájem převažuje nad zájmy subjektu údajů.[70] [71] Nejsou však vyloučeny ani zbylé případy uvedené v čl. 6 GDPR. Správce (zaměstnavatel) dodržuje zásady zpracování osobních údajů [72] a zejména zpracovává osobní údaje svých zaměstnanců vždy v rozsahu nezbytně nutném, především za účelem nastoupení do zaměstnání a jeho

[64] ZEMANOVÁ ŠIMONOVÁ, Hana. *Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů*. Bulletin advokacie, č. 9/2017, s. 25 a násl.
[65] Stanovisko WP 29 (WP 249) č. 2/2017 ze dne 8. 6. 2017 ke zpracování osobních údajů na pracovišti.
[66] Tamtéž.
[67] Čl. 6 odst. 1 písm. b) GDPR.
[68] Čl. 6 odst. 1 písm. c) GDPR.
[69] § 5 ZZOÚ.
[70] Čl. 6 odst. 1 písm. f) GDPR.
[71] Recitál 47 GDPR.
[72] Viz čl. 5 odst. 1 GDPR – zákonnost, korektnost a transparentnost (písm. a)), účelové omezení (písm. b)), minimalizace údajů (písm. c)), přesnost (písm. d)), omezení uložení (písm. e)), integrita a důvěrnost (písm. f)).

skončení, vedení personální, mzdové, odvodové nebo daňové agendy, evidence docházky, bezpečnosti ochrany zdraví při práci či vedení agendy pracovních úrazů. Vzhledem k výše uvedenému se v pracovní smlouvě a jiných pracovněprávních dokumentech po zaměstnanci souhlas se zpracováním osobních údajů nevyžaduje, naopak se jedná o postup, který je v rozporu s GDPR. Vzhledem k problematice nadbytečného vyžadování souhlasu se zpracováním osobních údajů a nesprávnému plnění informační povinnosti vydal stanovisko i ÚOOÚ. Postup, kdy správce vyžaduje po subjektu údajů souhlas se zpracováním osobních údajů, je tak pro subjekty osobních údajů poněkud matoucí v tom smyslu, že subjekt údajů může nabýt dojmu, že poskytnutí údajů není povinné a takový souhlas může v budoucnu odvolat. Správce však takovým počínáním subjekt údajů uvádí v omyl, co se týče zákonného důvodu zpracování osobních údajů a dále se dopouští porušení informační povinnosti.[73]

Přesto však můžeme v pracovněprávních vztazích výjimečně najít situace, na které se vztáhne zákonný důvod zpracování osobních údajů na základě udělení souhlasu se zpracováním osobních údajů. Souhlas je využíván v případě, kdy zpracování osobních údajů nespadá pod žádný jiný zákonný důvod uvedený v čl. 6 odst. 1 písm. b – f) GDPR. Půjde tak například o případ, kdy zaměstnavatel chce na své sociální sítě zveřejnit fotografie zaměstnanců z firemní akce (večírek, teambuilding). Zveřejnění takových fotografií má čistě reportážní účel,[74] nelze zde shledat účel (propagaci) zaměstnavatele ani nejde o žádné plnění povinností vyplývajících z pracovní smlouvy. Souhlas se poté vyžaduje vždy k jasně stanovenému účelu. Nemůže se jednat o „generální“ souhlas.[75]

[73] Stanovisko ÚOOÚ č. 3/2014, srpen 2014 k nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti, s. 2-3.
[74] V takových případech se uplatní především § 84 občanského zákoníku „*Zachytit jakýmkoliv způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.“*
[75] PATTYNOVÁ, Jana, SUCHÁNKOVÁ, Lenka, ČERNÝ, Jiří, a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. Praha: Leges, 2018. ISBN 978-90-7502-288-2, s. 103.

2 Povinnosti zaměstnavatele a práva zaměstnance

V této kapitole budu vycházet především z GDPR, neboť procesy zpracování osobních údajů, a s tím související povinnosti správce (zaměstnavatele) a práva subjektu údajů (zaměstnanců) spadají pod tuto právní úpravu. Předchozí právní úpravy mimo jiné kladly rovněž důraz na povinnosti zaměstnavatele a práva zaměstnanců. Ačkoliv GDPR přináší pár změn a klade celkově větší důraz na ochranu osobních údajů a procesy zpracování těchto údajů, nemůže být pro zaměstnavatele, kteří věnovali této oblasti pozornost již v minulosti, tato problematika žádným velkým překvapením.

2.1 Povinnosti zaměstnavatele

Jak již bylo zmíněno v předchozí kapitole, s účinností GDPR vznikají pro správce nové povinnosti a nové instituty, které zaměstnavatel musí promítnout do svých procesů ať se týkají budoucích, současných či bývalých zaměstnanců. Vzhledem k cíli práce se budu věnovat jenom vybraným aspektům, které se promítají do pracovněprávních vztahů.

Na prvním místě zaměstnavatel musí dodržovat zásady zpracování osobních údajů a zákonnost takového zpracování, což není žádnou novinkou (viz kapitola 1.2.6). Jak již bylo uvedeno, obecně je klíčové vytyčit účel, respektive z jakého důvodu dochází ke zpracování osobních údajů, což úzce souvisí se zásadou transparentnosti.[76]

2.1.1 Informační povinnost

V pracovněprávních vztazích je nutné komplexně informovat nejen zaměstnance, ale i uchazeče o zaměstnání, o tom, za jakým účelem, jakým způsobem, v jakém rozsahu, jak dlouho, kým a jaké osobní údaje jsou zpracovávány.[77] Dále je nutné informovat subjekty údajů o jejich právech vyplývajících ze zpracování osobních údajů. Za účelem splnění informační povinnosti vytvářejí zaměstnavatelé patřičné dokumenty – například interní směrnice, které o těchto skutečnostech subjekty údajů náležitě informují. Takové řešení naplňuje požadavek vyplývající z čl. 12 odst. 1 GDPR, který tvrdí, že:

[76] FIALA, Ondřej, GREPL, Jan, LICHNOVSKÝ, Ondřej. *GDPR: hmotné aspekty a procesní aspekty prakticky*. Právní praxe. Praha: C.H. Beck, 2019. ISBN 978-80-7400-762-0, s. 19.
[77] Čl. 13 GDPR.

„*Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých prostředků.“* V případě, že dojde k aktualizaci obsahu takového dokumentu, musí tuto skutečnost zaměstnavatel dát svým zaměstnancům taktéž na vědomí.[78] Správce musí zajistit, aby se komplexní informace o zpracování osobních údajů dostala opravdu ke všem zaměstnancům. Někdy nemusí postačit vystavení informace na určitém místě, neboť k němu nemusí mít všichni zaměstnanci přístup, zejména z důvodu, že nevyužívají k práci danou techniku.[79]

Informační povinnosti správce dle čl. 13 a 14 GDPR odpovídá právo na informace subjektu údajů.

Informační povinnost řeší nejen GDPR, ale též § 8 ZZOÚ. Uvedené ustanovení zmírňuje dopady GDPR v případech, kdy ke zpracování osobních údajů dochází na základě § 5 ZZOÚ, tedy za účelem plnění zákonné povinnosti nebo při výkonu veřejné moci. Správci tak mohou využít zjednodušený způsob plnění informační povinnosti, a to zveřejněním informace o zpracování osobních údajů způsobem umožňujícím dálkový přístup.[80]

2.1.2 Zabezpečení osobních údajů

Získané osobní údaje je třeba patřičně zabezpečit,[81] aby nedošlo k možnému úniku dat, a tím k porušení povinností vyplývajících z právních předpisů. Účelem zabezpečení je omezit možnost takového nežádoucího následku. GDPR nestanovuje jednotné řešení, což vzhledem k rozmanitosti správců a jejich činností není ani možné,[82] proto se v čl. 32 odst. 4 GDPR neurčitě zmiňuje o přijetí patřičných opatření. Předně by měl být každý zaměstnanec seznámen s nutností zabezpečení osobních údajů. Toto lze vyřešit vytvořením bezpečnostní směrnice.

Bezpečnostním opatřením může být uložení dokumentů obsahujících osobní údaje do uzamykatelné místnosti, případně do uzamykatelných skříní,

[78] MATES, Pavel (ed.), VALOUŠEK, Martin, FIALOVÁ, Eva, LECHNER, Tomáš, HÁLOVÁ, Markéta, SIVÁK, Jakub, SOVOVÁ, Olga, BRUNA, Eduard, BRUNOVÁ, Markéta. *Ochrana osobnosti, soukromí a osobních údajů.* Praha: Leges, 2019. ISBN 978-80-7502-346-9, s. 167.
[79] BOROVEC, David. Ochrana osobních údajů v personální praxi. Sborník přednášek z odborné konference Právní prostor 2018. *CODEXIS*® [online databáze]. Dostupné z https://app.codexis.cz
[80] VLACHOVÁ, Barbora. *Zákon o zpracování osobních údajů: komentář*. V Praze: C.H. Beck, 2019. Beckovy komentáře. ISBN 978-80-7400-760-6, s. 19.
[81] Čl. 32 GDPR
[82] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 49.

pokud se v místnosti pohybuje více osob, přičemž tyto osoby nemají stejná oprávnění s nakládáním osobních údajů. Zaměstnanci by měli dbát také na „politiku čistého stolu“, kdy při dlouhodobém opuštění pracoviště uloží veškeré neveřejné informace na uzamykatelné místo. Dalším bezpečnostním prvkem lze shledat i využití bezpečnostní služby a zajištění zázemí zaměstnavatele různými bezpečnostními systémy. Vzhledem k využívání elektronických vymožeností je třeba přijmout patřičná bezpečnostní opatření i na poli výpočetní techniky. Obecně lze konstatovat, že základem je pravidelné zálohování dat, neboť ztráta dat může mít dalekosáhlé negativní následky. V současné technicky vyspělé době není nijak neobvyklé, že zaměstnanci mají možnost využívat při své práci mobilní telefony, počítače a jinou elektroniku, a tím pádem je jim umožněn přístup například na sdílený disk či intranet. I v případě sdíleného disku by patřičné složky obsahující některé osobní údaje měly být omezeny v přístupu. Například osobní spisy zaměstnanců by neměly být volně přístupné, což vyplývá i z § 312 odst. 2 zákoníku práce, který stanovuje, že k osobnímu spisu má obecně přístup vedoucí zaměstnanec, který je nadřízen konkrétnímu zaměstnanci. Pokud by tento osobní spis nebyl náležitě zabezpečen, odpovídal by tak zaměstnavatel za porušení povinnosti vyplývající z § 312 zákoníku práce. Z rozhodnutí ÚOOÚ čj. UOOU-00742/13-83 ze dne 8. 3. 2013 vyplývá, že není žádoucí, aby byl využíván tzv. „zdvojený přístup“, přičemž *„zdvojený přístup neumožňuje ověřit a zjistit, který zaměstnanec prováděl zápisy, změny či čtení osobních údajů, a tedy z povahy věci vystavuje správce riziku, že nebude schopen v případě zneužití osobní údaje zjistit a prokázat, kdo ze zaměstnanců se takového jednání dopustil.“* Každý zaměstnanec by se tak měl přihlašovat do systému skrze jedinečné přihlašovací údaje.

2.1.3 Ohlašovací povinnost

Jestliže však následkem nedostatečného zabezpečení dojde k poškození dat, je zaměstnavatel povinen se obrátit na dozorový orgán a ohlásit tuto skutečnost do 72 hodin od okamžiku, kdy se dozvěděl o porušení zabezpečení osobních údajů.[83] Porušením zabezpečení osobních údajů se dle čl. 4 odst. 12 GDPR má na mysli takové *„porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.“* Nutno

[83] Čl. 33 GDPR.

doplnit fakt, že se správce nemusí obracet na dozorový orgán pokaždé, když dojde k nějakému porušení zabezpečení. Správce informuje dozorový orgán pouze tehdy, pokud by takové porušení mělo za následek riziko pro práva a svobody fyzických osob. V tomto případě se jedná o tzv. ohlašovací povinnost správce.

2.1.4 Oznamovací povinnost

Kromě ohlašovací povinnosti má správce povinnost oznamovací. Pokud totiž dojde k porušení zabezpečení osobních údajů subjektu, je správce kromě nahlášení dozorovému orgánu povinen oznámit tuto skutečnost také konkrétně poškozenému subjektu údajů dle čl. 34 GDPR. I zde, jako v případě ohlašovací povinnosti, se vyžaduje zvýšená míra rizikovosti pro práva a svobody fyzických osob.

Správce má oznamovací povinnost nejen vůči subjektům údajům, ale dle čl. 19 GDPR také vůči jednotlivým příjemcům, kterým jsou zpřístupněny osobní údaje, a to v případě uplatnění práva na opravu či doplnění, práva na výmaz a práva na omezení zpracování. Správce taktéž informuje subjekt údajů o těchto příjemcích, pokud takovou informaci požaduje. Pokud má příjemce přístup do databáze správce, může tak správce dle § 9 ZZOÚ splnit oznamovací povinnost vůči takovému příjemci pouhou změnou osobních údajů v evidenci.

2.2 Práva zaměstnance

Povinnostem správce, coby zaměstnavatele na druhé straně, odpovídají práva zaměstnanců, kteří jsou vůči zaměstnavatelům v pozici subjektu údajů. Tato práva úzce souvisejí se zásadou transparentnosti vyjádřenou v čl. 5 odst. 1 písm. a) GDPR. K uplatňování těchto práv může zaměstnavatel vytvořit pro zaměstnance patřičné formuláře, které zaměstnanec vyplní a následně se s formulářem obrátí na zaměstnavatele.

2.2.1 Právo na přístup k osobním údajům

Dále GDPR upravuje v čl. 15 právo na přístup k osobním údajům. Tento článek umožňuje subjektům údajů kontrolu nad zpracováním osobních údajů. V případě výše zmíněné informační povinnosti, která je uskutečňována z pozice správce aktivně, tedy správce nečeká na žádný podnět od subjektu údajů k podání informací. Kdežto u práva subjektu údajů na přístup k osobním údajům je třeba

vyvinutí iniciace ze strany subjektu údajů. Bez iniciace není správce povinen konat. Cílem je získání od zaměstnavatele potvrzení, zda o daném zaměstnanci zpracovává osobní údaje. Případnou negativní odpověď, tedy že zaměstnavatel dané osobní údaje nezpracovává, je zaměstnavatel povinen sdělit zaměstnanci. Pokud osobní údaje zaměstnavatel zpracovává, vzniká zaměstnanci právo získat přístup k těmto osobním údajům a k informacím uvedených v čl. 15 odst. 1 GDPR. Jedná se tak například o informace ohledně účelu zpracování, kategorii dotčených osobních údajů či kategorii příjemců, kteří mají přístup k osobním údajům dotčeného zaměstnance. Žádost o poskytnutí informací může podat subjekt opakovaně, přičemž je třeba mít na vědomí čl. 12 GDPR, který dává správci jakousi ochranu před četnými a šikanózními žádostmi.[84] Součástí práva na přístup k osobním údajům je i žádost o poskytnutí kopie zpracovávaných osobních údajů. Speciálním ustanovením vůči čl. 15 GDPR je § 312 zákoníku práce, který v odst. 3 vymezuje právo zaměstnance nahlížet do svého osobního spisu, přičemž si může ze svého spisu činit výpisky nebo si pořizovat stejnopisy dokladů, a to vše na náklady zaměstnavatele.[85]

2.2.2 Právo na opravu

Zaměstnavatel aktivně nezjišťuje aktuálnost ani nežádá o revizi osobních údajů poskytnutých ze strany zaměstnance.[86] Vzhledem k účelu zpracování osobních údajů v pracovněprávních vztazích je důležité, aby zaměstnavatel disponoval správnými údaji. Oprava osobních údajů je právem zaměstnance dle čl. 16 GDPR, nejedná se tedy o povinnost. Zaměstnavatel se tak vůči nesprávným informacím může „pojistit“ přijetím vhodného opatření, například zakotvením povinnosti zaměstnance hlásit zaměstnavateli případné změny v osobních údajích, které podléhají zpracování, v pracovní smlouvě.[87]

[84] MATES, Pavel (ed.), VALOUŠEK, Martin, FIALOVÁ, Eva, LECHNER, Tomáš, HÁLOVÁ, Markéta, SIVÁK, Jakub, SOVOVÁ, Olga, BRUNA, Eduard, BRUNOVÁ, Markéta. *Ochrana osobnosti, soukromí a osobních údajů.* Praha: Leges, 2019. ISBN 978-80-7502-346-9, s. 173.
[85] ZEMANOVÁ ŠIMONOVÁ, Hana. *Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů*. Bulletin advokacie, č. 9/2017, s. 25 a násl.
[86] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN: 978-80-7554-152-9, s. 138.
[87] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 79.

2.2.3 Právo na výmaz

Právo na výmaz neboli „právo být zapomenut“ zakotvené v čl. 17 GDPR je formulováno jako právo subjektu údajů na to, aby správce vymazal osobní údaje týkající se daného subjektu údajů. Dle Morávka právo na výmaz není novinkou, ačkoliv se někdy nesprávně za novinku, kterou přineslo GDPR, považuje, ale jedná se o součást právní úpravy na ochranu osobních údajů, přičemž „*rozdíl oproti předchozí právní úpravě spočívá, jako i v jiných oblastech, v konkretizaci institutu a ve větší míře kazuistiky právní úpravy.*“[88]

Nesprávným výkladem práva na výmaz je taková intepretace, kdy zaměstnanec má právo kdykoliv žádat výmaz osobních údajů, které se ho týkají.[89] Nejedná se o právo absolutní. Limity tohoto práva se promítají do čl. 17 GDPR, ve kterém jsou uvedeny důvody, pro které má správce povinnost osobní údaje bez zbytečného odkladu vymazat. Tyto důvody se neuplatní v případě výjimek z povinnosti výmazu, které jsou specifikovány v čl. 17 odst.3 GDPR, například povinnost výmazu se neuplatní, pokud je zpracování nezbytné pro splnění právní povinnosti. Typickým důvodem v pracovněprávních vztazích je naplnění účelu, pro které byly osobní údaje shromážděny nebo zpracovány. Půjde tak o případy, kdy po skončení pracovního poměru uplyne doba uchování patřičných dokumentů obsahujících osobní údaje a zaměstnavatel tak tyto dokumenty bude moci zlikvidovat. Po skončení pracovního poměru je nutné odstranit osobní údaje bývalého zaměstnance i z webu či sociálních sítí zaměstnavatele, neboť tyto zveřejněné údaje již nepodléhají svému prvotnímu účelu.

V předešlých kapitolách jsem se již zmiňovala o výjimečnosti poskytnutí souhlasu se zpracováním osobních údajů v pracovněprávních vztazích. V těchto případech je tedy možné vymazat osobní údaje na základě odvolání takového souhlasu v souladu s čl. 17 odst. 1 písm. b) GDPR. Odvolání souhlasu lze vztáhnout i na takového uchazeče o zaměstnání, který nebyl úspěšný na pohovoru, ale v souvislosti s přetrvávajícím zájmem o práci dal souhlas ke zpracování osobních údajů vyplývajících z životopisu za účelem kontaktování uchazeče v případě

[88] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN: 978-80-7478-139-1, s. 247.
[89] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 80.

uvolnění místa.[90] Pro náležité naplňování tohoto práva je na místě, aby zaměstnavatel přijal patřičná opatření. Tím může být vytvoření informativního dokumentu, který stanovuje pravidla pro pravidelnou a správnou likvidaci nepotřebných dokumentů obsahujících osobní údaje a dále pověření určitého zaměstnance, který bude mít tuto náplň práce na starost.

2.2.4 Právo na omezení zpracování

Omezením zpracování se dle čl. 4 odst. 3 má na mysli „*označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu.“* Od likvidace se tak omezení liší dočasností. V čl. 18 GDPR jsou taxativně uvedeny případy, kdy má subjekt údajů možnost uplatnit právo na omezení zpracování.[91] Pokud subjekt údajů uplatnil právo na omezení zpracování osobních údajů, mohou být nadále tyto osobní údaje zpracovávány pouze se souhlasem subjektu údajů nebo z důvodu určení, výkonu nebo obhajoby právních nároků a z důvodu ochrany práv jiné fyzické nebo právnické osoby.[92] V praxi se uplatnění takového práva reflektuje například dočasným odstraněním údajů z internetových stránek (nesprávných kontaktních údajů osoby), do té doby, než se nepřesnost odstraní.[93] V oblasti pracovněprávních vztahů takovým příkladem bude například úraz zaměstnance v areálu zaměstnavatele, přičemž se však nejedná o pracovní úraz. Zaměstnanec pro potřeby uplatnění práva na pojistné plnění z důvodu vzniku škodné události potřebuje záznam o úraze. V tomto případě by zaměstnanec žádal o omezení podle čl. 18 odst. 1 písm. c) GDPR.[94]

2.2.5 Právo na přenositelnost údajů

Právo na přenositelnost údajů je novým aktivním právem subjektu údajů. *„Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat*

[90] Tamtéž, s. 80-81.
[91] Viz čl. 18 odst. 1 GDPR – subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit (písm.a)), zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití (písm.b)), správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků (písm. c)), subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody převažují nad oprávněnými důvody subjektu údajů (písm. d)).
[92] Čl. 18 odst. 2 GDPR.
[93] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN: 978-80-7554-152-9, s. 141-142.
[94] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 81.

tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil." Jedná se pouze o případy, kdy je zpracování osobních údajů založeno na souhlasu nebo jde o zpracování založené smlouvou a takové zpracování se provádí automatizovaně.[95] Důležitým požadavkem je zde poskytnutí údajů ve strukturovaném, běžně používaném a strojově čitelném formátu.

K problematice přenositelnosti osobních údajů vydala WP 29 pokyn týkající se práva na přenositelnost údajů. Účelem tohoto institutu je zejména posílení moci subjektu údajů, které spočívá v tom, že subjekty údajů mohou se svými osobními údaji manipulovat jednodušeji. Problém u interpretace čl. 20 GDPR může nastat v části „poskytnuté subjektem údajů". Jak vyplývá z pokynu WP 29, je třeba tuto část vykládat z širšího hlediska. Půjde tak o případy, kdy správce získal údaje od subjektu údajů na základě aktivního a vědomého jednání subjektu údajů, a dále o takové údaje, které byly získány subjektem údajů na základě používání služby nebo zařízení.[96]

Právo na přenositelnost údajů však v oblasti pracovněprávních vztahů moc využití nenalezne, vztáhne se pouze na situace, kdy zaměstnavatel zpracovává automatizovaně osobní údaje na základě smlouvy, jejíž je subjekt údajů stranou.

2.2.6 Právo vznést námitku

Právo vznést námitku je specifikováno v čl. 21 GDPR jako právo subjektu údajů vznést námitku proti zpracování osobních údajů, které se jej týkají ze dvou zákonných důvodů dle čl. 6 GDPR, a to z důvodu, kdy je zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu, anebo pokud správce zpracovává osobní údaje pro účely svých oprávněných zájmů. V pracovněprávních vztazích tak typicky půjde o námitky proti zpracování za účelem oprávněných zájmů zaměstnavatele. Zaměstnanec tak může vznést námitku proti takovému zpracování, pokud má pochybnost, zda je v konkrétní věci skutečně přítomen onen oprávněný zájem zaměstnavatele. Při posuzováni oprávněného zájmu zaměstnavatele je nutné brát v potaz i právo zaměstnance na soukromí, které leží na druhé misce vah, a využít v tomto případě princip proporcionality. Na základě testu proporcionality, přičemž se poměřují práva zaměstnance na jedné straně a zájmy zaměstnavatele na

[95] Čl. 20 GDPR.
[96] Stanovisko WP 29 (WP 242) ze dne 13. 12. 2016, revidované a přijaté dne 5. dubna 2017 pokyny týkající se práva na přenositelnost údajů.

straně druhé, zaměstnavatel vyhodnotí, zda zpracování rozporovaných osobních údajů odpovídá stanovenému účelu a zda je rozsah zpracování údajů pro naplnění tohoto účelu nezbytný. Test proporcionality je interpretační metodou, ke které se Ústavní soud poprvé vyjádřil v nálezu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94. Zaměstnavatel by se měl držet zásady minimalizace osobních údajů a zbytečně nezpracovávat osobní údaje, které nejsou třeba pro naplnění stanoveného účelu. Pokud je zaměstnanec se svojí námitkou úspěšný, vzniká mu právo na výmaz dle čl. 17 odst. 1 písm. a) GDPR, respektive zaměstnavatel dané osobní údaje musí přestat zpracovávat pro daný účel. Čl. 21 odst. 4 GDPR rozvádí, že je možné vznést námitku proti zpracování osobních údajů pro statistické účely.

2.2.7 Právo nebýt předmětem automatizovaného individuálního rozhodování včetně profilování

Automatizované individuální rozhodování včetně profilování rozvíjí čl. 22 GDPR, který ve svém prvním odstavci stanovuje, že: „*Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.“* To však neplatí, pokud je rozhodnutí nezbytné k uzavření nebo plnění smlouvy nebo je povoleno právem EU nebo členského státu vztahující se na správce, anebo je takové rozhodnutí založeno na výslovném souhlasu subjektu údajů. [97] V pracovněprávních vztazích k automatizovanému zpracování osobních údajů zpravidla docházet nebude vzhledem k právnímu postavení mezi zaměstnancem a zaměstnavatelem.[98]

[97] Čl. 22 odst. 2 GDPR.
[98] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 84.

3 Zpracování osobních údajů v jednotlivých fázích pracovního poměru

V této kapitole se blíže zaměřím na zpracování osobních údajů v jednotlivých fázích pracovního poměru. Ke zpracování osobních údajů dochází totiž nejen v rámci pracovního poměru, ale také před vznikem a po skončení takového pracovního poměru.

3.1 Zpracování osobních údajů před vznikem pracovního poměru

Zákoník práce upravuje dle § 1 písm. d) rovněž vztahy vznikající před vznikem pracovněprávního vztahu. Z pohledu zaměstnavatele se jedná o důležitou fázi, neboť díky této fázi dochází k výběru zaměstnance. Ke konečnému rozhodnutí, který z uchazečů o zaměstnání je pro zaměstnavatele tím nejvhodnějším, jsou zapotřebí informace o dané osobě. Zaměstnavatel je však při získávání a obecně zpracování těchto informací omezen pravidly stanovenými právními předpisy, a to zejména GDPR, ZZOÚ, zákoníkem práce a zákonem o zaměstnanosti.

Ve fázi před vznikem pracovního poměru se zaměstnavatel nevyhne zpracování osobních údajů uchazečů o zaměstnání. Takové zpracování může provádět i bez souhlasu uchazečů v souladu s čl. 6 odst. 1 písm. b) GDPR, neboť se jedná o takové zpracování, které lze podřadit pod nezbytná opatření před uzavřením pracovní smlouvy. V odborné literatuře je zastáván i názor, že ke zpracování dochází v souladu s čl. 6 odst. 1 písm. f) GDPR, tedy ke zpracování osobních údajů dochází na základě oprávněného zájmu zaměstnavatele.[99] Pokud je proces výběru formalizován a je upraven právním předpisem, například zákonem o úřednících územně samosprávných celků, přichází v úvahu i právní titul vyplývající z čl. 6 odst. 1 písm. c) GDPR, tedy splnění právní povinnosti.[100] Zaměstnavatel je na prvním místě povinen dodržovat zásadu minimalizace osobních údajů, která je uvedena v čl. 5 odst. 1 písm. c) GDPR. Zaměstnavatel by podle tohoto ustanovení neměl žádat uchazeče o zaměstnání o jakékoliv údaje, ale pouze o ty, které jsou

[99] MATES, Pavel (ed.), VALOUŠEK, Martin, FIALOVÁ, Eva, LECHNER, Tomáš, HÁLOVÁ, Markéta, SIVÁK, Jakub, SOVOVÁ, Olga, BRUNA, Eduard, BRUNOVÁ, Markéta. *Ochrana osobnosti, soukromí a osobních údajů*. Praha: Leges, 2019. ISBN 978-80-7502-346-9, s. 204.
[100] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 329.

přiměřené účelu zpracování. Na úrovni zákonné úpravy pak zákoník práce v § 30 odst. 2 ve své podstatě opakuje, že zaměstnavatel smí vyžadovat od uchazeče jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy, přičemž tyto údaje „*je třeba vykládat jako všechny údaje, které jsou nutné ke svobodnému a vážnému rozhodnutí zaměstnavatele o tom, že s konkrétním zaměstnancem uzavře pracovní poměr“*.[101]

Informace o daném uchazeči zaměstnavatel získává především prostřednictvím životopisů, případně motivačních dopisů a dalších osobních dokumentů. Nabízí se otázka, zda je zaměstnavatel oprávněn čerpat informace z veřejně dostupných profilů na sociálních sítí. Obecně platí, že zaměstnavateli nic nebrání v tom vzít v úvahu i tyto informace. Takové jednání by mělo být vždy přiměřené a korektní, což by mělo zahrnovat i náležité informování uchazeče o využívání takových sociálních sítí k získání informací. Ze širokého spektra sociálních sítí, které se v dnešní době nabízí, s ohledem na § 30 odst. 2 zákoníku práce se jeví jako nejpříznivější platforma LinkedIn, která obsahuje profesní údaje o registrovaných uživatelích.[102] Naopak hojně rozšířené sítě jako Facebook nebo Instagram, jež uživatelé využívají ke sdílení svého soukromí, ať již se jedná o nejrůznější fotografie, či osobní postoje, mohou uchazeče „diskvalifikovat“, neboť na základě zveřejněného, mnohdy velice osobního obsahu, si může zaměstnavatel o dané osobě udělat v horším případě negativní „obrázek“. Otázkou zůstává, jak se proti takovému nezákonnému „vyřazení“ může uchazeč bránit, neboť otázka prokazování bude v praxi problematická. *„Zaměstnavatelé by se neměli domnívat, že pouhá veřejná dostupnost osobního profilu na sociálních sítích jim dovoluje zpracovávat tato data pro své vlastní účely. Pro takové zpracování je potřeba mít právní důvod, jako třeba oprávněný zájem.“* [103] Jinými slovy o zpracování osobních údajů se nejedná v případě, kdy si zaměstnavatel bude chtít jen ověřit pravdivost informací uvedených v životopise uchazeče a za tímto účelem použije sociální sítě. Naopak o zpracování už by se jednalo v případech, kdyby byly

[101] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN: 978-80-7478-139-1, s. 377.
[102] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 116-119.
[103] Stanovisko WP 29 (WP 249) č. 2/2017 ze dne 8. 6. 2017 ke zpracování osobních údajů na pracovišti.

informace zjištěné ze sociálních sítí zaznamenány.[104] V každém případě se již jedná o jakousi formu sledování ze strany zaměstnavatele.

Po skončení výběrového řízení nemusí být nutně všechny osobní údaje neúspěšných uchazečů odstraněny. Pro lepší objasnění, jak zaměstnavatel může nakládat s těmito údaji, lze rozdělit zpracovávání osobních údajů neúspěšných uchazečů na dvě skupiny. Co se týče zákonného důvodu zpracování těchto údajů, ani v jednom případě logicky nebude dále figurovat zákonný důvod zpracování dle čl. 6 odst. 1 písm. b) GDPR.

Do první skupiny budou patřit ti neúspěšní uchazeči, na které lze uplatnit další zpracování za některým ze slučitelných účelů dle čl. 6 odst. 4 GDPR a § 6 ZZOÚ a takové zpracování bude probíhat na základě čl. 6 odst. 1 písm. f) GDPR, tedy na základě oprávněného zájmu zaměstnavatele. Jedná se tak například o situace, kdy zaměstnavatel potřebuje mít k dispozici údaje za účelem obrany v antidiskriminačním sporu. Na základě stejného právního titulu lze zpracovávat informace neúspěšného uchazeče také po dobu běhu zkušební doby, která běží úspěšně přijatému uchazeči o zaměstnání, avšak s ohledem na vysokou fluktuaci pracovníků na dané pracovní pozici je pravděpodobné, že ve zkušební době může dojít k odchodu pracovníka ze zaměstnání. Neúspěšnému uchazeči však tato skutečnost musí být sdělena při výběrovém řízení a tento zmíněný postup lze aplikovat pouze pokud tento neúspěšný uchazeč nevyjádřil nesouhlas s dalším možným kontaktováním ze strany zaměstnavatele.[105]

Druhou skupinu tvoří neúspěšní uchazeči o zaměstnání, jejichž osobní údaje jsou uchovávány a zpracovány v jakési databázi potenciálních zaměstnanců za účelem pozdějšího oslovení. Zaměstnavatel v tomto případě již bude muset od neúspěšného uchazeče získat souhlas se zpracováním osobních údajů v souladu s čl. 6 odst. 1 písm. a) GDPR. Zaměstnavatel není oprávněn nadále archivovat životopisy těch neúspěšných uchazečů, kteří neposkytli zaměstnavateli svobodný

[104] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 119.
[105] LIŠKUTÍN, Tomáš. *Ochrana soukromí a osobních údajů uchazečů o zaměstnání (GDPR).* Praktická personalistika, č. 1-2/2018, s. 13 a násl.

souhlas ke zpracování osobních údajů. Tyto životopisy je zaměstnavatel povinen skartovat nebo vymazat.[106]

Zaměstnavatel se také může setkat s nevyžádanými životopisy. Jedná se o situace, kdy není inzerované žádné pracovní místo, přesto však uchazeči o zaměstnání z vlastní iniciativy zašlou zaměstnavateli svůj životopis. Pokud zaměstnavatel takový životopis hned odstraní, bude se jednat pouze o nahodilé shromáždění osobních údajů a neuplatňují se zde postupy vyplývající z GDPR.[107] Zaměstnavatel se však nevyhne informační povinnosti ani v případě, že uchazeč o zaměstnání vysloví souhlas se zpracováním osobních údajů již ve svém životopise. Pokud se zaměstnavatel rozhodne uchovat si nadále informace o takovém uchazeči, musí splnit informační povinnost dle čl. 13 GDPR. To lze vyřešit například odkazem na patřičný dokument nacházející se na webových stránkách zaměstnavatele nebo e-mailem, ve kterém bude uchazeč patřičně informován o podrobnostech zpracování osobních údajů.

Obecně zaměstnavatel smí po uchazečích o zaměstnání vyžadovat adresní a identifikační údaje (jméno, příjmení, datum narození, adresa bydliště, e-mailová adresa, telefonní číslo) a dále údaje, které souvisejí s vykonáváním potenciální práce, a svědčí tak o způsobilosti uchazeče (např. dosažené vzdělání, zdravotní způsobilost, jazykové dovednosti).[108] Vždy by měl být zaměstnavatel schopen odpovědět na to, proč je požadovaný údaj pro něj potřebný, zda je nezbytný pro daný účel. Osobní údaje, které uchazeč o zaměstnání poskytnul sám bez vyzvání nad rámec, by zaměstnavatel neměl vůbec zpracovávat a takové osobní informace by měly být odstraněny. To je však zaměstnavateli porušováno např. formou vstupních dotazníků, neboť obsahují údaje, které by zaměstnavatel neměl vyžadovat vůbec, anebo se jedná o údaje, které jsou potřebné až po uzavření pracovní smlouvy,[109] například rodné číslo či údaj o exekucích. Případný osobní dotazník by tak měl v zásadě splňovat zásadu minimalizace osobních údajů. V praxi se stává, že jsou dotazníky univerzální či neaktualizované. Taková praxe není příliš

[106] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 331,
[107] LIŠKUTÍN, Tomáš. *Ochrana soukromí a osobních údajů uchazečů o zaměstnání (GDPR).* Praktická personalistika, č. 1-2/2018, s. 13 a násl.
[108] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 109-112.
[109] JANEČKOVÁ, Eva, BARTÍK, Václav. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN: 978-80-86131-96-2, s. 51-52.

žádoucí, neboť tak může docházet k vyzývání vyplnění více údajů o uchazeči o zaměstnání, než je reálně potřeba pro danou pozici.[110]

Podrobněji okruh zakázaných informací vymezuje zákon o zaměstnanosti v § 12 odst. 2, ve kterém se hovoří o fázi výběru zaměstnanců, přičemž zakazuje zaměstnavateli vyžadovat při výběru zaměstnanců informace týkající se národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení, sexuální orientace a dále informace, které odporují dobrým mravům, a osobní údaje, které neslouží k plnění povinností zaměstnavatele. Na žádost uchazeče o zaměstnání je zaměstnavatel povinen prokázat potřebnost požadovaného osobního údaje. Zaměstnavatel takové informace nesmí získávat ani prostřednictvím třetích osob. Informace o trestněprávní bezúhonnosti v tomto ustanovení není uvedena, neboť s ohledem na některá pracovní místa bude pro potenciálního zaměstnavatele tato informace relevantní.[111]

Další omezení vyplývají i z § 316 odst. 4 zákoníku práce, který demonstrativně vymezuje, které informace zaměstnavatel nesmí vyžadovat od zaměstnance ani od třetích osob, přičemž za použití argumentace a fortioti a maiori ad minus lze toto ustanovení vztáhnout i na uchazeče o zaměstnání. Zaměstnavatel nesmí vyžadovat informace, které bezprostředně nesouvisejí s výkonem práce, a to zejména informace o těhotenství, rodinných a majetkových poměrech, sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách nebo hnutích, příslušenství k církvi nebo náboženské společnosti a trestněprávní bezúhonnosti. Informace uvedené v tomto ustanovení lze rozdělit do dvou skupin, a to informace absolutně zakázané a informace relativně zakázané.

Údaje o sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách nebo hnutích a příslušnosti k církvi nebo náboženské společnosti podléhají režimu absolutního zákazu, neboť zaměstnavatel tyto údaje nesmí nikdy vyžadovat. Údaje o těhotenství, rodinných a majetkových poměrech a trestněprávní bezúhonnosti se nacházejí v režimu relativního zákazu, kdy zaměstnavatel je oprávněn tyto údaje požadovat, pokud je pro to dán věcný důvod

[110] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 111.
[111] BARTÍK, Václav, JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi (vybrané problémy)*. 4. vydání. Praha: Wolters Kluwer ČR, a. s., 2016. ISBN 978-80-7552-141-5, s. 138.

spočívající v povaze práce, která má být vykonávána, a jestliže je tento požadavek přiměřený. [112] Zaměstnavatel je oprávněn vyžadovat údaj o těhotenství ženy v případě prací zakázaných těhotným ženám s ohledem na vyhlášku č. 180/2015 Sb., o pracích a pracovištích, které jsou zakázány těhotným zaměstnankyním, zaměstnankyním, které kojí, a zaměstnankyním-matkám do konce devátého měsíce po porodu, o pracích a pracovištích, které jsou zakázány mladistvým zaměstnancům, a o podmínkách, za nichž mohou mladiství zaměstnanci výjimečně tyto práce konat z důvodu přípravy na povolání (vyhláška o zakázaných pracích a pracovištích). Předložení výpisu z trestního rejstříku bývá v praxi zaměstnavatelem často požadováno, avšak ne vždy je tento požadavek legitimní. Tento požadavek je oprávněný jen tam, kde se trestněprávní bezúhonnost skutečně vyžaduje, například u pracovníků, kteří manipulují s penězi.[113] Údaje týkající se rodinných a majetkových poměrů jsou spíše mířeny až na samotný průběh pracovního poměru.

3.2 Zpracování osobních údajů v průběhu pracovního poměru

V průběhu pracovního poměru by se zaměstnavatel s ohledem na povinnosti vyplývající z právních předpisů jen těžko obešel bez zpracování osobních údajů svých zaměstnanců. Logicky tak sjednáním pracovní smlouvy dochází ke zpracování osobních údajů v širším rozsahu, než tomu je ve fázi před vznikem pracovního poměru. Osobní údaje zaměstnanců, které musí zaměstnavatel zpracovávat, lze rozdělit na dvě skupiny, a to na osobní údaje, které zpracovává zaměstnavatel obligatorně, a na osobní údaje, které zpracovává fakultativně.

Každý zaměstnavatel je povinen vést mzdovou a personální agendu. Tato agenda je značně roztříštěna a vztahuje se na ni několik právních předpisů. Mezi stěžejní právní předpisy patří zákoník práce, zákon o zaměstnanosti, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, z. č. 155/1995 Sb., o důchodovém pojištění a zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, zákon

[112] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN: 978-80-7478-139-1, s. 378-379.
[113] VALENTOVÁ, Klára, PROCHÁZKA, Jan, JANŠOVÁ, Marie, ODROBINOVÁ, Veronika, BRŮHA, Dominik a kol. *Zákoník práce.* Komentář. Praha: C. H. Beck, 2018. ISBN 978-80-7400-534-3, s. 71.

č. 586/1992 Sb., o daních z příjmů, zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), z. č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád). Zaměstnavatel musí mít vždy na paměti zásady zpracování osobních údajů vyplývající z GDPR, zejména pak čl. 5 odst. 1 písm. b), přičemž osobní údaje musí být „*shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.“* Zaměstnavatel nesmí v rámci vedení personální a mzdové agendy vyžadovat a zpracovávat informace vyplývající z § 316 odst. 4 zákoníku práce (viz kapitola 3.1). [114] Zákoník práce naproti tomu rovněž stanovuje obligatorní zpracování osobních údajů, a to vedení pracovní doby dle § 96, povinnost vést knihu úrazů dle § 105 odst. 2 a dále vést evidenci zaměstnanců, u nichž byla uznána nemoc z povolání dle § 105 odst. 6.

Dále § 312 odst. 1 zákoníku práce opravňuje zaměstnavatele vést osobní spis zaměstnance. Osobní spis může být veden v písemné či elektronické podobě, anebo v obou těchto formách. Tento spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu. Obsahem spisu jsou jak údaje, které byly o zaměstnanci shromážděny již v rámci výběrového řízení, tedy před zavřením pracovní smlouvy, tak i údaje shromážděné v průběhu pracovního poměru. Jedná se tak zejména o údaje identifikační a kontaktní, údaje nezbytné pro splnění povinností zaměstnavatele na úseku daňové správy a sociálního zabezpečení, písemnosti týkající se odměňování, dohody vztahující se k pracovnímu poměru, doklady prokazující proškolení zaměstnance v různých oblastech, listiny týkající se vyslání na pracovní cesty, rozvržení pracovní doby apod. [115] Problém může nastat při zpracování citlivých údajů. Typickou problematikou jsou lékařské zprávy a posudky. Zaměstnavatel bude jistě moci zpracovávat lékařské posudky o způsobilosti zaměstnance k práci. Jiné je to ovšem v případě invalidního zaměstnance, kdy by zaměstnavatelé neměli v osobních spisech uchovávat lékařské zprávy týkající se invalidity. Zde postačí pro plnění právních povinností pouze posudek o tom, že je zaměstnanec invalidní. Lékařské zprávy budou naopak potřeba uchovávat v případě, kdy se zaměstnanci stane

[114] LIŠKUTÍN, Tomáš. *Ochrana soukromí a osobních údajů uchazečů o zaměstnání (GDPR) – I. část.* Praktická personalistika, č. 3-4/2018, s. 7 a násl.
[115] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 349-351.

pracovní úraz nebo nemoc z povolání. Účelem zpracování těchto dokumentů jsou zejména oprávněné zájmy zaměstnavatele.[116]

V následujícím odstavci bych se ráda krátce věnovala mzdovým údajům a platu zaměstnance. Ačkoliv údaj o mzdě nebo platu není zařazen ve zvláštní kategorii osobních údajů, je všeobecně ve společnosti vnímán velice citlivě. Zaměstnanci tak očekávají, že zaměstnavatelé budou tyto údaje náležitě chránit, aby k nim neměly přístup neoprávněné osoby. Pokud není takový údaj součástí pracovní smlouvy, je stanoven ve mzdovém/platovém výměru, který je součástí osobního spisu zaměstnance. K informacím o mzdě/platu má přístup pouze omezený okruh osob, který má povinnost mlčenlivosti. Avšak na základě právního předpisu mohou být tyto informace zpřístupněny dalším osobám, dle § 312 odst. 2 zákoníku práce se jedná o orgán inspekce práce, Úřad práce ČR, ÚOOÚ, soud, státní zástupce, policejní orgán, Národní bezpečnostní úřad a zpravodajské služby. Co se týče případného zveřejňování těchto údajů, tak se zveřejňováním údajů o mzdě v praxi nebývá problém. Jinak je tomu v případě zveřejňování údajů o platu. Zejména platy vyšších úředníků a funkcionářů jsou vystaveny zájmu široké veřejnosti.[117] Obecně platí, že právo na informace je ústavně garantované dle čl. 17 Listiny, přičemž toto právo je přímo uplatnitelné na základě Listiny. Pro účely zajištění práva veřejnosti na informace[118] byl přijat zákon č. 106/1999 Sb., o svobodném přístupu k informacím. Informační právo je v našem právním řádu postaveno zejména na soudních rozhodnutích. Poskytované informace však mohou na druhé straně zasáhnout do ochrany osobních údajů, zejména pak pokud jde o žádost o informaci o platu zaměstnance. Prvním klíčovým rozhodnutím v otázce zveřejňování platů zaměstnanců veřejné správy bylo rozhodnutí Nejvyššího správního soudu ze dne 27. 5. 2011, sp. zn. 5 As 57/2010-79, které vyjasnilo otázku ohledně zveřejňování platů zaměstnanců, kterým je vyplácena odměna z veřejných prostředků. „*Informace o konkrétní odměně takového konkrétního zaměstnance, a to včetně její výše, je proto povinný subjekt povinen poskytnout v rozsahu vymezeném § 8b odst. 3 citovaného zákona.“* Ústavní soud v rozhodnutí ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16-4 vyslovil, že údaje o platu lze poskytnout

[116] BOROVEC, David. Ochrana osobních údajů v personální praxi. Sborník přednášek z odborné konference Právní prostor 2018. *CODEXIS*® [online databáze]. Dostupné z https://app.codexis.cz
[117] BARTÍK, Václav, JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi (vybrané problémy)*. 4. vydání. Praha: Wolters Kluwer ČR, a. s., 2016. ISBN 978-80-7552-141-5, s. 163-164.
[118] 16/0 senátní návrh zákona o svobodném přístupu k informacím a o změně dalších zákonů.

pouze s ohledem na právo na soukromí a jen za podmínky zvláštního testu, kdy se musí zejména zkoumat, zda se informace týká veřejného zájmu.

3.3 Zpracování osobních údajů po skončení pracovního poměru

Skončením pracovního poměru nedochází ihned k ukončení zpracování osobních údajů bývalého zaměstnance. Co se týče skončení pracovního poměru, je nutné mít na paměti zejména povinnost zpracovávat osobní údaje korektně, zákonným a transparentním účelem, v přiměřeném, relevantním, omezeném a nezbytném rozsahu. Zaměstnavatel některé osobní údaje potřebuje po nějakou dobu i po skončení pracovního poměru, zejména pro potřeby hájení práv zaměstnavatele, vypořádání práv a povinností a pro povinné uchovávání dokumentů. Stanovená doba je u různých dokumentů různě dlouhá, vše vychází z předmětných právních předpisů, například evidenční listy dle § 35a odst. 4 písm. d) zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, je zaměstnavatel povinen uchovávat mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění po dobu 30 kalendářních roků následujících po roce, kterého se týkají. Zaměstnavatel takové informace nemůže zlikvidovat ani na základě využití práva na výmaz ze strany bývalého zaměstnance. Zpravidla se další uchovávání osobních údajů děje již z jiného právního titulu než pro účely plnění smlouvy, jako tomu bylo u předchozích fází pracovního poměru. Pokud však s některým zaměstnancem byla v průběhu pracovního poměru podepsána konkurenční doložka, právním titulem pro zpracování osobních informací zde bude i nadále plnění smlouvy.[119] V případě existence konkurenční doložky je zaměstnavatel oprávněn monitorovat za účelem ověření dodržování doložky profil bývalých zaměstnanců na sociální síti LinkedIn.[120]

Pokud zaměstnavatel uchovává osobní údaje bývalých zaměstnanců pro potřeby hájení svých práv a doložení plnění svých zákonných povinností, musí vzít v potaz obecnou promlčecí lhůtu 3 roky u majetkových práv. Stejná lhůta je stanovena i pro zánik odpovědnosti zaměstnavatele u řady přestupků. S ohledem na tuto promlčecí lhůtu je pro zaměstnavatele vhodné, aby patřičné dokumenty uchovával 4 roky, pokud se vezmou v potaz všechny procesní okolnosti. V případě

[119] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 102 a 157.
[120] Stanovisko WP 29 (WP 249) č. 2/2017 ze dne 8. 6. 2017 ke zpracování osobních údajů na pracovišti.

včasného zahájení přestupkového řízení nebo soudního sporu se doba uchování údajů může ještě prodloužit.[121] Dalším důvodem, proč zaměstnavatel uchovává informace i po skončení pracovního poměru, mohou být diskriminační spory, ve kterých funguje obrácené důkazní břemeno, kdy je na zaměstnavatelovi, aby prokázal, že nedošlo k porušení zásady rovného zacházení.[122]

Nepotřebné informace zaměstnavatel musí v přiměřené době po skončení pracovního poměru zlikvidovat, například životopis nebo různá osvědčení, jejichž uchovávání ztratilo pro zaměstnavatele dále na významu. Co se týče likvidace informací, je vhodné vybrat takový způsob skartace, který zaručuje, že osobní údaje nebudou dále zpracovávány. Zaměstnavatel může pověřit skartací například specializovanou firmu, která se pak na základě smlouvy stává zpracovatelem.[123] Za likvidaci údajů se považuje i anonymizace údajů.[124]

Bez zbytečného odkladu je nutné zlikvidovat i fotografie, které byly předmětem zpracování, například portrétní fotografie daného bývalého zaměstnance, která byla umístěna na webových stránkách zaměstnavatele. Čistě reportážní fotografie není nutné likvidovat.[125]

Při skončení pracovního poměru vydá zaměstnavatel zaměstnanci dle § 313 odst. 1 zákoníku práce potvrzení o zaměstnání, případně dle § 313 odst. 2 zákoníku práce potvrzení o výši průměrného výdělku. Dále je povinný vydat písemně důvod rozvázání pracovního poměru a o dokumenty o dalších skutečnostech rozhodných pro posouzení nároku na podporu v nezaměstnanosti.

Další dokument, který zaměstnavatel může vypracovat na žádost odcházejícího zaměstnance, je pracovní posudek. V § 314 zákoníku práce je zakotveno právo zaměstnance žádat od zaměstnavatele vydání posudku o pracovní činnosti. „*Pracovním posudkem jsou veškeré písemnosti týkající se hodnocení práce zaměstnance, jeho kvalifikace, schopnosti a další skutečnosti, které mají*

[121] LIŠKUTÍN, Tomáš. *Ochrana soukromí a osobních údajů zaměstnanců (GDPR) – II. část.* Praktická personalistika, č. 5-6/2018, s. 8 a násl.
[122] § 133a zákona č. 99/1963 Sb., občanský soudní řád.
[123] JANEČKOVÁ, Eva, BARTÍK, Václav. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 120-122.
[124] LIŠKUTÍN, Tomáš. *Archivace dokladů v osobních spisech zaměstnanců po skončení zaměstnání.* Praktická personalistika č. 3-4/2019, rubrika Odpovídáme na dotazy čtenářů, s. 48-49.
[125] ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s.164.

vztah k výkonu práce.[126] *Jiné informace o zaměstnanci než ty, které mohou být obsahem pracovního posudku (odstavec 1 věta druhá), je zaměstnavatel oprávněn o zaměstnanci podávat pouze s jeho souhlasem, nestanoví-li zvláštní právní předpis jinak.“*[127] Informace uvedené v pracovním posudku mají povahu osobních údajů a vytvořením pracovního posudku dochází ke zpracování osobních údajů a dopadá na něj obecná právní úprava na ochranu osobních údajů obsažena v GDPR a ZZOÚ. To samé platí i pro potvrzení o zaměstnání a s ohledem na tuto skutečnost není možné, aby došlo k dohodě mezi zaměstnavatelem a zaměstnancem ohledně toho, že nějaký údaj uvedený v § 313 odst. 1 zákoníku práce nebude v potvrzení o zaměstnání uveden. Ze stejného důvodu není možné ani rozšířit rozsah údajů v rámci potvrzení o zaměstnání.[128] Dále § 315 zákoníku práce stanoví postup zaměstnance, pokud nesouhlasí s obsahem potvrzení o zaměstnání nebo pracovního posudku, přičemž v případě nesouhlasu se může zaměstnanec obrátit na zaměstnavatele a požadovat úpravu patřičného dokumentu. Pokud zaměstnavatel nevyhoví zaměstnanci, má zaměstnanec možnost se obrátit na civilní soud a domáhat se tak úpravy pracovního posudku touto cestou. Zaměstnanec musí brát v potaz to, že soud je omezen žalobním petitem, tedy zaměstnanci je možné přisoudit jen to, co zaměstnanec (žalobce) v žalobě uplatňuje.

[126] § 314 odst. 1 zákoníku práce.
[127] § 314 odst. 2 zákoníku práce.
[128] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 357.

4 Sledování zaměstnanců

V oblasti sledování zaměstnanců na jedné straně figuruje ochrana majetkových zájmů zaměstnavatele či zajištění bezpečnosti na pracovišti, a na druhé straně ochrana osobních práv zaměstnanců, zejména soukromí, osobních údajů a listovního tajemství. Z toho důvodu je důležité postupovat podle principu proporcionality, a poměřovat tak tyto dvě naproti sobě stojící práva v každém konkrétním případě. Sledováním se má na mysli taková forma kontroly ze strany zaměstnavatele, která trvá delší dobu nebo se systematicky opakuje prostřednictvím určitého systému či prostředku. Za sledování se považuje i kontrola v reálném čase. O sledování naopak nepůjde, pokud je monitorovací prostředek zřízen primárně za jiným účelem a zaměstnanec je skrze něj kontrolován ad hoc.[129] Za sledování se také nepovažuje namátková kontrola zaměstnance, například jednorázový vstup do e-mailové schránky zaměstnance, neboť zde nedochází k aplikaci zákoníku práce.

Sledování zaměstnanců se týká pouze § 316 zákoníku práce, který čítá čtyři odstavce, přičemž všechny lze považovat ve své podstatě za kogentní s částečnou výjimkou odstavce prvého, který umožňuje zaměstnavateli určitá jednání. Co se týče aplikace právních předpisů, na prvním místě zde figuruje zákoník práce jakožto speciální právní předpis. Pokud nějakou otázku neupravuje zákoník práce a současně se jedná o zpracování osobních údajů, aplikuje se právní úprava ochrany osobních údajů, tedy GDPR a ZZOÚ. Ve všech případech se však podpůrně použije občanský zákoník, neboť každý zásah do soukromí se týká ochrany osobnosti dle občanského zákoníku.[130] Ustanovení § 81 občanského zákoníku mimo jiné tvrdí, že ochrany požívá i soukromí člověka. Dále § 84 až 90 občanského zákoníku rozvádí blíže soukromí a podobu člověka, jakým způsobem lze zachytit podobu člověka, pořizovat zvukové či obrazové záznamy soukromého života. Významným ustanovením pro pracovněprávní vztahy ve spojení s problematikou sledování je také § 88 odst. 1 občanského zákoníku, který říká, že: „*Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.“*

[129] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 377.
[130] NONNEMANN, František. *Soukromí na pracovišti*. Právní rozhledy, 7/2015, s. 229 a násl.

První odstavec se týká dozoru zaměstnanců. Dozorem se nerozumí monitoring, který je přípustný jen výjimečně.[131] Zaměstnanci mohou využívat výrobní a pracovní prostředky zaměstnavatele pro svou osobní potřebu pouze se souhlasem zaměstnavatele. Zaměstnavatel je oprávněn přiměřeným způsobem dozorovat, zda nedochází k využívání těchto prostředků bez jeho souhlasu. Pod neurčitým pojmem „přirozeným způsobem" si lze představit takový způsob, který je vzhledem k okolnostem vhodným prostředkem k dosažení účelu. Zaměstnavatel může kontrolu provádět i mimo pracovní dobu, avšak s ohledem na fakt, že zaměstnanci mimo pracovní dobu svědčí větší míra soukromí. Kontrola zákazu nemůže být však prováděna libovolně.[132] Ochrana osobnosti zaměstnance se neuplatňuje v závažných případech, kdy zaměstnanec v pracovní době využívá ve větším rozsahu prostředky zaměstnavatele k uspokojení osobního zájmu.[133] Což je podloženo i judikaturou, například v rozsudku Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011, kdy se v tomto případě zaměstnanec bránil argumentem, že sledování ze strany zaměstnavatele bylo neoprávněné, avšak soud dospěl k závěru, že zaměstnavatel v souladu se zákonem, konkrétně § 316 odst. 1 zákoníku práce, přiměřeným způsobem kontroloval dodržování zákazu užívání prostředků zaměstnavatele k osobním potřebám zaměstnance, který se v tomto případě zabýval téměř 103 hodin v jednom měsíci z celkových 168 pracovních hodin mimopracovní činností, zejména sledováním nevhodných stránek. V konečném důsledku je toto soudní rozhodnutí významné tím, že se zabývá ve své podstatě kontrolou užívání prostředků zaměstnavatele, a nikoliv sledováním zaměstnanců jako takovým. Nejvyšší soud ve svém rozsudku také vysvětlil rozdíl mezi odst. 1 a 2 § 316 zákoníku práce. První odstavec se vztahuje ke kontrole zaměstnance, zda nevyužívá prostředky zaměstnavatele bez jeho souhlasu. Zaměstnavatel má tak právo kontrolovat dodržování tohoto zákazu a v případě zjištění, že zaměstnanec tento zákaz nedodržuje, si opatřit důkaz o tomto nedodržování. Druhý odstavec se již vztahuje jen na případy, kdy zvláštní povaha činnosti zaměstnavatele umožňuje sledování zaměstnance, který užívá prostředky zaměstnavatele s jeho souhlasem. V dané kauze bylo předmětem to, zda zaměstnanec navštěvoval internetové

[131] Stanovisko ÚOOÚ č. 2/2009, únor 2009 ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.
[132] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 375-376.
[133] JOUZA, Ladislav. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. Bulletin advokacie, č. 6/2014, s. 26 a násl.

stránky, které osvědčují mimopracovní činnost, a nikoliv to, které konkrétní internetové stránky jsou navštěvovány. V uvedené kauze byla míra zásahu do soukromí zaměstnance zanedbatelná, což prokazuje i odmítnutí následné ústavní stížnosti usnesením Ústavního soudu ze dne 7. 11. 2012, sp. zn. I. ÚS 3933/12.[134] Na závěr je na místě ještě podotknout, že pokud v rámci dozoru bude docházet ke zpracování osobních údajů zaměstnance, uplatní se zde taktéž právní úprava na ochranu osobních údajů.

Odstavec druhý § 316 již řeší sledování zaměstnance v pravém slova smyslu. Při výkladu tohoto ustanovení je opět nutno myslet na případy, kdy má narušování soukromí povahu zpracování osobních údajů, neboť se musí respektovat i úprava na ochranu osobních údajů, přičemž v takovém případě musí být splněn právní titul podle čl. 6 odst. 1 písm. f) GDPR.[135] „*Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci*.“ [136] Státní inspekce pro úřad práce má za to, že závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele je potřeba zkoumat v rámci konkrétního zaměstnavatele a konkrétního pracoviště. Tento závažný důvod není dán při poskytování běžných služeb.[137] Závažným důvodem může být například provoz technologie, u které existuje riziko, že by tento provoz mohl způsobit škodu na majetku nebo zdraví zaměstnanců či třetích osob. Důvodem zavedení sledovacího opatření je pak zejména ochrana života a zdraví nebo ochrana majetku zaměstnavatele nebo i jiných osob nacházejících se ve sledovaných prostorech.[138]

---

[134] BARANCOVÁ, Helena, OLŠOVSKÁ, Andrea (eds.). *Pracovné právo v digitalnej době*. Praha: Leges, 2017. ISBN 978-80-7502-259-2, s. 166.
[135] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 377-378.
[136] § 316 odst. 2 zákoníku práce.
[137] Monitorování zaměstnanců na pracovišti kamerovým systémem. *Suip.cz* [online]. 2014. [cit. 8. 3. 2020]. Dostupné z: http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance/monitorovani-zamestnancu-na-pracovisti-kamerovym-systemem-pridano-7-4-2014
[138] VALENTOVÁ, Klára, PROCHÁZKA, Jan, JANŠOVÁ, Marie, ODROBINOVÁ, Veronika, BRŮHA, Dominik a kol. *Zákoník práce.* Komentář. Praha: C. H. Beck, 2018. ISBN 978-80-7400-534-3, s. 974-975.

Dále dle § 316 odst. 3 platí, že pokud je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů, musí zaměstnavatel informovat své zaměstnance o rozsahu kontroly a způsobech jejího provádění, a to již před zahájením činnosti. Zákon nezmiňuje formu takového informování. Jistě je možné zaměstnance informovat i ústní formou, avšak pro případ možného pozdějšího prokázání splnění této povinnosti se tato forma nemusí jevit jako účinné řešení.

Čtvrtý odstavec svým obsahem nezapadá mezi předchozí odstavce a z legislativně-technického hlediska by měl být spíše od zbytku ustanovení oddělen. [139] Tomuto odstavci jsem se blíže věnovala již v kapitole ohledně zpracování osobních údajů před vznikem pracovněprávního poměru (kapitola 3.1.). Stručně lze shrnout, že toto ustanovení je ve své podstatě z větší části kogentní, lze se od něj odchýlit jen ve prospěch zaměstnance a určuje omezení rozsahu zjišťování údajů. Tento zákaz nemůže prolomit ani vyslovení souhlasu ze strany zaměstnance.

O jakési sledování mimo pracovní dobu lze hovořit v případě sledování zaměstnanců prostřednictvím sociálních sítí. Tyto nekorektní praktiky zaměstnavatelů budou v praxi jen těžko prokazatelné, mnohdy nemusí mít zaměstnanec ani tušení, že se něco takového děje. Nejúčinnější obranou je dle mého názoru prevence. Tedy pokud možno nezveřejňovat příliš osobní informace, mít povědomí o sledujících osobách či přátelích na těchto sítích, a pokud je to možné, přepnout veřejné účty na soukromé.

Vzhledem k tomu, že je právní úprava v oblasti sledování zaměstnanců velmi strohá, tak mantinely mezi právem zaměstnavatele na ochranu svých majetkových zájmů a právem zaměstnance na ochranu soukromí určují z velké části soudní rozhodnutí, což může mít za následek právní nejistotu adresátů právních norem. Avšak pevné mantinely dle mého názoru stanovit nelze, neboť ke každému případu je nutné přistupovat individuálně a vzít v potaz všechny okolnosti, které se k dané situaci pojí.

Současná doba digitalizace naskytla zaměstnavatelům nové formy sledování svých zaměstnanců, respektive umožnila širší zásah do soukromého

[139] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3, s. 371.

života zaměstnanců. Mezi nejrozsáhlejší sledovací opatření, ke kterým zaměstnavatelé přistupují, patří zejména kamerové systémy, monitoring pohybu zaměstnanců prostřednictvím GPS lokalizátoru umístěném na služebním vozidle, kontrola pohybu na internetu, sledování e-mailové korespondence či telefonní komunikace. Dále je možné se setkat s méně invazivními formami monitoringu v tom smyslu, že hlavní funkcí nastolení takového opatření není trvalý monitoring. Jedná se o mystery shopping nebo systémy určené k evidenci docházky zaměstnanců, například čipové karty. Naopak mezi nejpřísnější opatření sloužící ke sledování zaměstnanců patří monitorovací zařízení, která umožňují sledovat zaznamenávání stisku jednotlivých kláves či pohyb myší (tzv. keylogger) nebo monitoring pracovní plochy počítače. Tyto formy sledování již značně zasahují do soukromí zaměstnance a nejsou ani běžně využívány.[140] Úřad pro ochranu osobních údajů doporučuje zaměstnavatelům vytvořit vnitřní předpis, kterým stanoví jasná pravidla monitoringu, případně tato pravidla doporučuje zakomponovat do pracovního řádu.[141]

Otázkou může být, jak se může zaměstnanec bránit vůči zaměstnavateli v případě, kdy se domnívá, že praktiky zaměstnavatele jsou nepřípustné a výrazně zasahují do soukromí zaměstnance. Vše se bude odvíjet podle aplikované právní úpravy na daný postup zaměstnavatele. Na prvním místě je jistě vhodné, aby zaměstnanec předně došel za svým nadřízeným, případně za zaměstnavatelem, a pokud možno se situaci pokusil vyřešit tou nejjednodušší cestou, tedy domluvou. Mnohdy může být do soukromí zaměstnance zasahováno neúmyslně. Především zde však záleží na zaměstnanci, neboť zaměstnanec se může přirozeně bát o svoji pozici a v řadě případů se raději uchýlí k tomu, že svá práva „pro jistotu“ hájit nebude z obavy o možné následné problémy, například zhoršení vztahů na pracovišti. Bude-li zaměstnanec svá práva přece jenom hájit, může se obrátit na kontrolní orgán, a to na Státní úřad inspekce práce, který může zkontrolovat například oprávněnost kamerového systému. Pokud takovým zásahem do práva zaměstnance dochází ke zpracování osobních údajů, má zaměstnanec jakožto subjekt údajů dle GDPR nově právo vznést u zaměstnavatele námitku proti

[140] POLONI, Marek. Nové trendy ve sledování zaměstnanců. *Pravniprostor.cz* [online]. 2020 [cit. 29. 2. 2020]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/nove-trendy-ve-sledovani-zamestnancu

[141] Stanovisko ÚOOÚ č. 2/2009, únor 2009 ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.

zpracování (viz kapitola 2.2.6). Bude-li zaměstnanec nespokojený s vyřízením své námitky, může se pak obrátit na dozorový orgán ÚOOÚ.

Možností, jak může zaměstnavatel sledovat zaměstnance, je tedy nespočet a jistě v budoucnu budou další formy sledovacích opatření přibývat. Následně v dalších podkapitolách se zaměřím na aplikaci § 316 odst. 2 a 3 zákoníku práce, případně i právní úpravy ochrany osobních údajů na standardní metody sledování, přičemž na závěr uvedenu i jednu metodu z kategorie méně invazivních forem sledování.

4.1 Sledování pomocí kamerových systémů

Mezi jednu ze standardních forem sledování zaměstnanců patří využívání kamerových systémů. Kamerovým systémem je myšlena i pouze jedna kamera. Kamerové systémy lze rozdělit na monitoring bez pořízení záznamu a monitoring se záznamovým zařízením. Obecně platí, že je zakázáno využívat kamerové systémy v prostorech určených k odpočinku a hygieně zaměstnance a kamery nesmí být naměřeny na osobu zaměstnance.[142]

Zaměstnavatelé využívají kamerové systémy ke dvěma účelům. Prvním z nich je instalace kamerových systémů za účelem sledování zaměstnanců, zda plní své pracovní povinnosti a zda nejsou na pracovišti porušovány zákazy, jako například zákaz kouření či konzumace alkoholu. Druhým účelem je ochrana majetku, tedy zaměstnavatel instaluje kamerové zařízení k předcházení krádeží.[143]

Kamerovým systémem nepochybně dochází k otevřenému sledování zaměstnanců. I přesto, že se v zákoníku práce nachází řada ustanovení,[144] která zdůvodňují využívání kontrolních mechanismů, využívání kamerových systémů lze použít pouze při uplatnění výjimky dle § 316 odst. 3 zákoníku práce, konkrétně výjimky spočívající ve zvláštní povaze činnosti zaměstnavatele. V jiném případě by se tak jednalo o porušení zákoníku práce, případně také porušení úpravy ochrany

[142] Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012-49.
[143] JANEČKOVÁ, Eva, BARTÍK, Václav. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti.* Praha: Linde, 2011. ISBN: 978-80-7201-850-5, s. 67.
[144] Srov. § 248 odst. 2 věta první zákoníku práce *„Zaměstnavatel je z důvodu ochrany oprávněn v nezbytném rozsahu provádět kontrolu věcí, které zaměstnanci k němu vnášejí nebi od něho odnášejí, popřípadě provádět prohlídky zaměstnanců.“*; § 301 písm. a) zákoníku práce *„Vedoucí zaměstnanci jsou dále povinni řídit a kontrolovat práci podřízených zaměstnanců a hodnotit jejich pracovní výkonnost a pracovní výsledky.“*

osobních údajů, pokud dochází ke zpracování osobních údajů. Pokud se zaměstnavatel vejde do těchto mantinelů, musí dále splnit povinnosti správce osobních údajů vyplývajících z právních úprav ochrany osobních údajů.[145] Je nutné mít však na paměti, že ani tato výjimka neopravňuje zaměstnavatele k neomezenému monitorování zaměstnanců. Jak už bylo uvedeno, zaměstnanec má i na pracovišti právo na určitou míru soukromí. *„Ze zásady přiměřenosti zpracování osobních údajů vyplývá, že tyto systémy lze použít v případě, že se jiná opatření směřující k prevenci, ochraně anebo zabezpečení fyzické nebo logické povahy, která nevyžadují pořizování obrazových záznamů ukáží být nedostatečnými a/nebo nepoužitelnými s ohledem na výše uvedené legitimní účely. Postup zpracovatele, který nadřadil zájem na ochraně před drobnými krádežemi, vandalstvím a případným excesem některého z návštěvníků nad právo na ochranu soukromí a osobního života, je nepřípustný a především neproporcionální.“*[146] Kamerový systém lze využít pouze v případě, kdy účelu, tedy ochrany práv a právem chráněných zájmů zaměstnavatele, nelze dosáhnout jinou cestou a tímto způsobem kontroly musí být do soukromí zaměstnanců zasahováno, pokud možno co nejméně. [147] Jinými slovy, ne vždy je na místě pořizovat kamerový systém, neboť lze využít i jiné zabezpečovací mechanismy, které mnohdy dokážou splnit svůj účel stejně tak dobře jako kamerové systémy, navíc s tím, že ve finále není tolik zasahováno do práv zaměstnance.

Kromě zákoníku práce se na provoz kamerového systému vztahuje také úprava ochrany osobních údajů. Je tomu tak u kamerových systémů se záznamovým zařízením, kdy dochází ke zpracování osobních údajů, pokud je vedle kamerového sledování také prováděn záznam pořizovaných záběrů za účelem identifikace fyzických osob v souvislosti s jejich určitým jednáním. Nutno podotknout, že fyzická osoba je identifikovatelná, pokud lze ze záznamu pochytit charakteristické rozpoznávací znaky, zejména obličej. Pořízený záznam nemusí však vždy dosahovat takové kvality, aby bylo následně možné určitou osobu plně identifikovat bez dalších doprovodných informací, které v daném záznamu

[145] JANEČKOVÁ, Eva, BARTÍK, Václav. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti.* Praha: Linde, 2011. ISBN: 978-80-7201-850-5, s. 69-70.
[146] Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012-49.
[147] *Provozování kamerových systémů*: *metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů*. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2012. ISBN 978-80-210-6017-3.

obsaženy nejsou. Pokud tento záznam nebude doplněn o doprovodné údaje, díky nimž lze následně danou osobu identifikovat, nelze takto získané údaje vztáhnout k určitému nebo určitelnému subjektu. Přestože některé osoby nebude možné v praxi identifikovat z těchto záznamu, musí se na celý proces nahlížet jako na zpracování údajů o identifikovatelných osobách,[148] což vyplývá i ze stanoviska WP 29 (WP 136) č. 4/2007. Bez následné možnosti identifikace osoby by takové kamerové systémy postrádaly smysl.

Z povahy věci je zřejmé, že kamerovým sledováním bez záznamu nevzniká zpracování osobních údajů a na tuto činnost se nevztahuje právní úprava ochrany osobních údajů vyplývající z GDPR a ZZOÚ, to však nevylučuje informační povinnost zaměstnavatele. Na tuto činnost se kromě zákoníku práce vztahuje občanský zákoník ve svých ustanoveních ohledně osobnosti člověka, konkrétně pak § 86 tvrdí, že nikdo nesmí zasáhnout do soukromí jiného, pokud k tomu nemá zákonný důvod, zejména pak sledovat jeho soukromý život nebo o tom pořizovat záznam. *„Pokud kamera slouží jako „prodloužené oko“, nemá se tak sledovaná osoba obracet na Úřad pro ochranu osobních údajů, nýbrž na soud s žalobou na ochranu osobnosti.“*[149] Ochrany se tak zaměstnanec může domoci prostřednictvím civilních soudů. Dle mého názoru tato forma sledování zasahuje do soukromí zaměstnance více než je tomu tak u sledování pomocí kamerového systému se záznamem, neboť u kamerového systému bez pořizování záznamu musí být neustále nějaká osoba, která sleduje dění na pracovišti a v případě krizové situace je oprávněna zasáhnout.

Instalací kamerového systému však nedochází ve všech případech ke sledování zaměstnanců dle zákoníku práce. Kamerové systémy mohou mnohdy pouze nahodile zachycovat zaměstnance, například jsou-li kamery instalovány za účelem střežení nějakého prostoru, kam zaměstnanci vstupují pouze v případě potřeby. V těchto případech se tedy neaplikuje ustanovení zákoníku práce ohledně

[148] VIDRNA, Jan, KOUDELKA, Zdeněk. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců*. Praha: C. H. Beck, 2013. ISBN 978-80-7400-453-7, s. 124-126.
[149] Veřejný ochránce práv. Kamerové systémy a ochrana osobních údajů. *Ochrance.cz* [online]. 2012 [cit. 2. 3. 2020]. Dostupné z: https://www.ochrance.cz/ochrana-osob-omezenych-na-svobode/aktuality-z-detenci/aktuality-z-detenci-2012/kamerove-systemy-a-ochrana-osobnich-udaju/

sledování zaměstnanců, ale jistě tu bude docházet ke zpracování osobních údajů, tudíž je nezbytné se zde řídit právní úpravou ochrany osobních údajů.[150]

Na závěr bych ráda zmínila rozhodnutí Nejvyššího správního soudu 10 As 245/2016 ze dne 20. 12. 2017, ve kterém se Nejvyšší správní soud vyjádřil zamítavě ohledně podané kasační stížnosti. Stěžovatelka v daném případě hájila oprávněnost umístění kamerového systému do přední části autobusu. Tato nainstalovaná kamera by snímala pouze obrazový záznam, avšak po celou dobu by sledovala řidiče autobusu a stevarda. Stěžovatelka spatřovala zákonnost zpracování osobních údajů zejména s odkazem na ochranu svých oprávněných zájmů, která je uvedena v § 5 odst. 2 písm. e) ZOOÚ[151]. Nejvyšší soud však namítl, že zpracování osobních údajů je třeba hodnotit dle zásady proporcionality. V této kauze se do rozporu na straně jedné dostává právo soukromí, na straně druhé právo na ochranu života a majetku. Test proporcionality však „ztroskotal" u kritéria potřebnosti, neboť k instalaci kamerového systému je obecně možno přistoupit až tehdy, kdy veškeré méně invazivní prostředky selhaly, anebo nebyly schopny naplnit vytyčený účel, který je sledován. Nejvyšší správní soud dovodil, že nepřetržitým pořizováním kamerového záznamu dochází k výraznému zásahu do soukromí monitorovaných osob a monitorování také může negativně ovlivnit pozornost řidičů. Žalovaný Městský soud vzal dále v potaz § 316 odst. 2 zákoníku práce a dospěl k závěru, že provoz autobusové dopravy nespadá do režimu zvláštní povahy činnosti zaměstnavatele. S tímto tvrzením se ztotožnil i Nejvyšší správní soud. Domnívám se, že je používání kamerových systémů na pracovištích nadužíváno. Je pochopitelné, že zaměstnavatel chce mít na jednu stranu jistotu a „klid na duši", že je jeho majetek dostatečně chráněn a díky kamerovému systému se záznamovým zařízením má taktéž zajištěné důkazní materiály, avšak na druhou stranu by se měl vcítit do pozice zaměstnance. Nikomu jistě není příjemné vědomí toho, že je pod neustálým dozorem. To může mít za následek vznik stresu u zaměstnanců a ten v dlouhodobém hledisku může nepříznivě ovlivnit pracovní výkon zaměstnance.

[150] NONNEMANN, František. *Soukromí na pracovišti*. Právní rozhledy, 7/2015, s. 229 a násl.
[151] „*Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.*"

4.2 Sledování korespondence

Podle čl. 13 Listiny nesmí nikdo porušit listovní tajemství ani tajemství jiných písemností a záznamů. Tajemství je zaručeno i zprávám podávaných telefonem, telegramem nebo jiným podobným zařízením. Pod pojmem „podobné zařízení“ si v současné době na prvním místě lze představit zejména elektronickou poštu. Listovní tajemství je možné porušit pouze v případech a způsobem, který stanoví zákon. Stanovisko ÚOOÚ č. 2/2009 tvrdí, že pro elektronické dokumenty platí stejná pravidla jako pro jiné písemnosti.

Listovní poštu je zaměstnavatel oprávněn otevřít jenom výjimečně, zejména v případech, kdy je zaměstnanec na pracovišti dlouhodobě nepřítomen (například z důvodu nemoci) a kdy by v případě nereagování na obsah listiny mohl přijít zaměstnavatel k újmě.[152] Zde je však nutné si vyjasnit, zda se jedná o písemnost pracovní či soukromou. Tuto skutečnost je možné mnohdy zjistit již přečtením informací na obálce. Soukromá zpráva je adresována primárně zaměstnanci, přičemž na prvním místě je na obálce uvedeno jeho jméno. Obdobně se postupuje i v případě e-mailových zpráv.[153]

V případě e-mailové korespondence je důležitá e-mailová adresa a její formát. Ačkoliv je doména ve vlastnictví zaměstnavatele, klíčovou roli zde hraje adresa. Tedy je-li adresa složena ze jména a příjmení zaměstnance, je e-mailová zpráva doručena na tuto adresu zprávou soukromou. Taková adresa je osobním údajem, který může zaměstnavatel zpracovávat i zveřejnit. Obecně konstruovaná adresa jako např. recepce@firma.cz, je považována za úřední elektrickou adresu, a to i v případě, že je tato schránka spravována pouze jedním zaměstnancem. Pro rozpoznávání, zda se jedná o soukromou či pracovní zprávu, se vychází z identifikačních znaků, jako je odesílatel, předmět zprávy a oslovení příjemce.[154]

K pravidelnému sledování elektronické pošty je však zapotřebí závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Ten může být shledán již v tom, zda zaměstnanec plní pracovní povinnosti a pravidelně

[152] HANÁK, Jakub. Právo zaměstnavatele na narušení listovního tajemství. *Pravniprostor.cz* [online]. 2020 [cit. 3. 3. 2020]. Dostupné z https://www.pravniprostor.cz/clanky/ustavni-pravo/pravo-zamestnavatele-na-naruseni-listovniho-tajemstvi
[153] Stanovisko ÚOOÚ č. 2/2009, únor 2009 ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.
[154] Tamtéž.

komunikuje se svými klienty nebo dodavateli. Zaměstnavatel však smí monitorovat pouze hlavičky e-mailových zpráv, neměl by se blíže seznamovat s obsahem těchto zpráv. Dále je nutné zaměstnance předem o tomto monitorování informovat. S obsahem e-mailových zpráv se může zaměstnavatel seznámit pouze výjimečně, pouze z důvodů povolených zákonem. Soukromou zprávu může přečíst jen tehdy, stejně jako u listinné korespondence, je-li to nezbytné k ochraně jeho práv či zamezení utrpění jeho zájmů. V tomto případě totiž zaměstnavatel hájí své ústavně garantované právo dle čl. 11 Listiny. Současně však musí být zřejmé dle hlavičky e-mailové zprávy, že obsah se bude týkat pracovních záležitostí, nikoliv osobního života zaměstnance. [155] Takovým monitoringem opět dochází ke zpracování osobních údajů, a proto se zde nepochybně uplatní i právní úprava ochrany osobních údajů.

Naopak o monitoring se nejedná v případě, kdy zaměstnavatel vstoupí pouze jednorázově do e-mailové schránky zaměstnance. Avšak i v tomto případě dochází ke zpracování osobních údajů a je třeba na tento postup aplikovat právní úpravu ochrany osobních údajů.

Zasažením práva zaměstnance na ochranu soukromého života a korespondencí se zabýval ESLP ve stěžejním rozsudku Bărbulescu proti Rumunsku č. 61496/08, který stanovil, že zaměstnavatelé mají povinnost předem upozornit zaměstnance na to, že jejich elektronická komunikace bude sledována. Dále k takovému sledování musí mít legitimní důvod. V této kauze byl zaměstnanec propuštěn ze zaměstnání, neboť využíval i přes zákaz Yahoo Messenger k soukromým účelům. V tomto případě docházelo k monitorování elektronické komunikace zaměstnance, ačkoliv zaměstnanec nebyl zaměstnavatelem vyrozuměn o povaze a rozsahu sledování. Jinými slovy zaměstnavatelé jsou nejen povinni informovat zaměstnance o možnosti monitorování elektronické korespondence, ale musí také předem vymezit způsob a rozsah provádění kontroly. Rozsudek s sebou přinesl i nastolení kritérií. Posuzující orgán, zejména pak vnitrostátní soud, by tak měl řešit otázky toho, zda byl zaměstnanec informován o sledování korespondence a jeho způsobu a rozsahu, v jakém rozsahu probíhalo sledování a v jaké míře bylo zasaženo soukromí zaměstnance, přičemž je třeba rozlišit mezi sledováním obsahu

[155] VALENTOVÁ, Klára, PROCHÁZKA, Jan, JANŠOVÁ, Marie, ODROBINOVÁ, Veronika, BRŮHA, Dominik a kol. *Zákoník práce.* Komentář. Praha: C. H. Beck, 2018. ISBN 978-80-7400-534-3, s. 978-979.

komunikace a sledováním pouhého přehledu aktivit. Posuzující orgán by se dále měl zabývat prostorovým a časovým omezením a otázkou oprávněnosti přístupu k výsledkům sledování. Mezi další kritéria patří zákonnost sledování komunikace a otázka subsidiarity, tedy zda bylo možné dosáhnout účelu i jinak než přímým zásahem do komunikace zaměstnance. Soud by měl posoudit důsledky, které vznikly sledovanému zaměstnanci, zda výsledky sledování zaměstnavatel využil pro stanovený cíl a dále je nutné posoudit to, zda měl zaměstnanec záruku toho, že zaměstnavatel před seznámením se s obsahem komunikace bude zaměstnance o tomto faktu informovat. Tento stěžejní rozsudek je aplikovatelný nejen na monitoring elektronické korespondence, ale i na další formy sledování zaměstnanců. [156]

4.3 Sledování telefonních hovorů

V návaznosti na předchozí podkapitolu je na místě krátce rozvést i problematiku sledování telefonních hovorů. K odposlechu telefonu na pracovišti se vyjádřil v minulosti ESLP ve svém rozsudku Halford proti Spojenému království, č. 20605/92, přičemž podle něj se telefonní hovory podřazují pod soukromý život a korespondenci ve smyslu čl. 8 Úmluvy. V případě telefonních hovorů je tedy zaručeno tajemství zpráv dle čl. 13 Listiny.

Pokud je zaměstnanci v rámci výkonu práce přidělen služební telefon i k soukromým účelům, dochází tak ze strany zaměstnavatele ke zpracování osobních údajů, neboť pro účely účetnictví musí shromažďovat faktury za telefonní hovory. Zaměstnavatel je tak legitimně oprávněn zpracovávat seznam hovorů, a to na základě analogie rozsudku Bărbulescu proti Rumunsku. K čemu již ale oprávněn není, je odposlech soukromých hovorů.

Monitoring pracovních hovorů podléhá § 316 odst. 2 zákoníku práce, přičemž je závažným důvodem spočívajícím ve zvláštní povaze zaměstnavatele. Záznam telefonních hovorů bude vždy osobním údajem, neboť zaměstnanec na základě takového záznamu bude vždy identifikovatelný.[157] Telefonní hovory jsou zaznamenávány typicky u call center či telefonních operátorů. Závažným důvodem

[156] BARANCOVÁ, Helena, OLŠOVSKÁ, Andrea (eds.). *Pracovné právo v digitalnej době*. Praha: Leges, 2017. ISBN 978-80-7502-259-2, s. 164-165 a 168.
[157] Stanovisko ÚOOÚ č. 5/2013, říjen 2013 pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů.

spočívajícím ve zvláštní povaze zaměstnavatele v tomto případě lze shledat plnění smluvních povinností a dle stanoviska ÚOOÚ č. 5/2013 je legitimním účelem také zvyšování kvality služeb. Pokud však zaměstnavatel bude odposlouchávat telefonní hovory, aniž by pořizoval záznam, nepoužije se v tomto případě úprava ochrany osobních údajů, neboť zde nedochází ke zpracování osobních údajů.

4.4 Sledování prostřednictvím GPS technologie

Technologie GPS umožňuje zjištění polohy a navigaci. Tato technologie se využívá zejména u dopravních prostředků, které byly zaměstnancům svěřeny pro výkon práce. Některé dopravní prostředky mohou být obzvlášť nákladné, proto účelem sledování je především ochrana majetkových zájmů zaměstnavatele, dále případně zajištění bezpečnosti řidičů či přepravovaných osob. Kromě toho GPS může zrychlit a ulehčit práci zaměstnancům, zejména co se týče komunikace, neboť díky této technologii může pracovník snadno zjistit, kde se nachází jeho kolega, což lze uvítat zejména v případě přepravy osob či věcí, kde významnou roli hraje čas.

S využíváním GPS technologie však dochází v mnoha případech k zásahu do soukromí sledovaného zaměstnance, proto by zaměstnavatel měl vždy postupovat s ohledem na právo a soukromí zaměstnanců. Aby sledování pomocí GPS naplňovalo § 316 odst. 2 zákoníku práce a jednalo se tak o sledování v pravém slova smyslu, musí být používání GPS soustavné a intenzivní. Sledování naopak nepředstavuje situace, kdy je pouze prostřednictvím GPS namátkově kontrolováno dané vozidlo, například zda se zaměstnanec skutečně nachází na určeném místě. V tomto případě ani nedochází ani ke zpracování osobních údajů.[158]

V souvislosti s využíváním tohoto sledovacího opatření dochází ve většině případů ke zpracování osobních údajů zaměstnance, neboť zaměstnavatel je schopen si vygenerovaná data spojit s jednotlivými zaměstnanci, a to ani nemusí docházet k přímému propojování těchto dat ke konkrétním zaměstnancům, postačí zde existence možnosti, že k propojení může dojít.[159] Z pohledu právní úpravy ochrany osobních údajů se jako právním titulem zpracování osobních údajů jeví zejména oprávněný zájem zaměstnavatele.

[158] RADIČOVÁ, Zuzana. *Monitoring zaměstnanců prostřednictvím GPS technologie.* Právní rozhledy, 21/2014, s. 736 a násl.
[159] Rozhodnutí ÚOOÚ zn. INSP1-3568/12-16 ze dne 3. 1. 2013.

Jedním z benefitů v rámci pracovněprávních vztahů může být svěření vozidla zaměstnanci i pro soukromé účely. Práva a povinnosti jsou v takovém případě upraveny dohodou o užívání daného vozidla. V této dohodě musí být zaměstnanec upozorněn, že je na vozidle nainstalováno navigační zařízení, které umožňuje určení aktuální polohy vozidla. Co se týče zpracování osobních údajů, bude zde i nadále figurovat právní titul „oprávněný zájem" zaměstnavatele. Zaměstnavatel se však musí nadále držet zásady minimalizace zpracování osobních údajů, tedy zpracování osobních údajů za účelem ochrany majetku, evidence jízd k prokázání daňové uznatelnosti výdajů na pohonné hmoty či oprávněnosti odpisů vozidla. Zaměstnavatel se nesmí uchýlit k soustavné kontrole, která by byla v rozporu s § 316 odst. 2 a 3 zákoníku práce.[160] Zaměstnavatel takovému jednání může předejít vypnutím sledovacího zařízení, pokud bude zaměstnanec absolvovat soukromou jízdu. V souvislosti s touto problematikou není na škodu zopakovat fakt, že mimo pracovní dobu náleží zaměstnanci větší právo na soukromí.

4.5 Mystery shopping

V posledních letech se tento méně invazivní typ kontroly těší oblibě. Jedná se o monitoring prostřednictvím utajované identity, přičemž určitá osoba se chová jako zákazník či klient, který má zájem o určitý produkt nebo službu. Primárním úkolem této osoby je, aby prostřednictvím určitých otázek, které klade pracovníkovi, zhodnotila správnost komunikace zaměstnance se zákazníky či klienty. V rámci mystery shoppingu se užívá také technika tzv. mystery calling, přičemž účelem této techniky je zjistit, jak si vedou zaměstnanci v komunikaci se třetími osobami prostřednictvím telefonu nebo e-mailu.[161]

Mystery shopping provádí třetí osoba tzv. „agent" na popud zaměstnavatele a uskutečňuje se formou utajeného sledování. V průběhu toho mohou být i nahrávány audionahrávky či videozáznamy. Pokud se jedná o opakující se činnost, naplňuje tento monitoring § 316 odst. 2 zákoníku práce, přičemž jako závažný důvod lze shledat, stejně jako nahrávání telefonních hovorů při provozu call center,

[160] Zaměstnavatelé: Úřad pro ochranu osobních údajů. *Uoou.cz* [online]. [cit. 6. 3. 2020] Dostupné z: https://www.uoou.cz/zamestnavatele/ds-5057
[161] KADLECOVÁ, Tereza. *Monitoring zaměstnanců*. Praktická personalistika č. 11-12/2015, s. 22 a násl.

zvyšování kvality poskytovaných služeb. Pokud se jedná o jednorázový nahodilý monitoring, toto ustanovení naplněno nebude.

Při provádění této formy kontroly dochází ke zpracování osobních údajů,[162] a to jak v případě opakující se činnosti, tak i v případě jednorázové kontroly. Ačkoliv zaměstnanec nebude vědět, kdy byla kontrola zahájena ani kdy skončila, nebude tato kontrola naplňovat znaky skrytého sledování, pokud tento zaměstnanec bude předem v souladu s právní úpravou ochrany osobních údajů informován, že k takovým formám kontroly bude v průběhu výkonu práce docházet a jak takové kontroly budou prováděny. Pokud tato skutečnost nebude předem oznámena, bude se jednat o sledování skryté. Dle Jakuba Morávka by ke skrytému sledování mělo docházet jenom výjimečně, neboť se jedná o invazivnější zásah do soukromí, než je tomu u otevřeného sledování.[163]

[162] NONNEMANN, František. *Soukromí na pracovišti*. Právní rozhledy, 7/2015, s. 229 a násl.
[163] MORÁVEK, Jakub. *Kontrola a sledování zaměstnanců – výklad k § 316 ZPr*. Právní rozhledy 17/2017, s. 573 a násl.

Závěr

Vzhledem k rozsáhlé problematice ochrany osobních údajů si diplomová práce kladla za cíl seznámit čtenáře s problematikou ochrany osobních údajů v pracovněprávních vztazích. O aktuálnosti tématu ochrany osobních údajů svědčí i množství relevantní odborné literatury a článků na toto téma, ze kterého jsem v průběhu práce čerpala. Nemohu opomenout ani stanoviska ÚOOÚ a WP29 (v současné době úlohu převzal Evropský sbor pro ochranu osobních údajů) jakožto další významné zdroje informací, neboť vydaná stanoviska těchto institucí pomáhají osvětlit problematické otázky. Dalším důležitým interpretačním vodítkem je i judikatura evropských i národních soudů. GDPR bylo přijato zejména z důvodu sjednocení právních úprav členských států EU, avšak v oblasti pracovněprávních vztahů tento účel naplněn nebude, protože čl. 88 GDPR umožňuje členským státům stanovit konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců. V ČR zatím nedošlo k přijetí žádných pravidel. Z pohledu pracovněprávních vztahů nová úprava GDPR nezměnila definice pojmů ani platné zásady ve vztahu k ochraně a zpracování osobních údajů, pouze zpřísnila a zpřesnila povinnosti správce. Přijetí GDPR má vliv i na monitoring zaměstnanců, zejména na požadavky zabezpečení osobních údajů zaměstnanců. Nově musí správce ohlašovat bezpečnostní incidenty dozorovému úřadu a dále oznámit subjektu údajů fakt, že je bezpečnost osobních údajů ohrožena či porušena. Subjekt údajů pak nově může využít práva na přenositelnost údajů nebo vznést námitku proti zpracování. Námitky proti zpracování lze využít také v případě sledování zaměstnanců, pokud současně dochází ke zpracování osobních údajů. Přijetím GDPR a jeho medializací došlo k větší motivaci zaměstnavatelů k úpravě vnitřních předpisů za účelem dosažení souladu s právní úpravou. Negativním důsledkem může být pak vyšší administrativní či finanční zátěž zaměstnavatelů.

V práci jsem věnovala pozornost zejména zvláštní kategorii osobních údajů neboli citlivým osobním údajům, přičemž definice této kategorie osobních údajů lze najít v GDPR, zákoníku práce a zákonu o zaměstnanosti, avšak ustanovení týkající se těchto pojmů spolu vzájemně nekorespondují. Dále byla větší pozornost věnována i souhlasu ke zpracování osobních údajů. S ohledem na nerovné postavení zaměstnance a zaměstnavatele není využití tohoto zákonného důvodu

dost dobře možné, proto své uplatnění nalezne jen ve výjimečných případech a zaměstnavatelé se tak musí opřít o jiný zákonný důvod. V pracovněprávních vztazích se jedná zejména o plnění právních povinností.

Majoritní část této práce byla věnována prostoru jednotlivým fázím pracovněprávního vztahu s důrazem na zpracování osobních údajů v těchto jednotlivých fázích. Pozornost byla věnována i problematice vyhledávání informací o uchazečích či zaměstnancích na sociálních sítích. Na závěr jsem se zaměřila vybraným institutům sledování zaměstnanců, kde jsem na různé situace aplikovala právní úpravu zákoníku práce a právní úpravu ochrany osobních údajů. Během zkoumání problematiky sledování zaměstnanců jsem dospěla k závěru, že aplikace právních předpisů není vždy na první pohled zcela jasná. Důvodem je strohá úprava v zákoníku práce, přičemž zde pak při následné aplikaci hraje roli zejména princip proporcionality. Vše závisí na konkrétní situaci a dále se situace odvíjí dle účelu zřízení sledovacího zařízení. Z toho důvodu si myslím, že i přesto je úprava v zákoníku práce dostačující, neboť s ohledem na spektrum pracovních pozic a množství situací není možné vše zakomponovat do zákonné úpravy. Ve všech případech se uplatní obecná úprava ochrany soukromí, tedy občanský zákoník. V některých případech se dále aplikuje pouze zákoník práce, pokud v rámci sledování nedochází dále ke zpracování osobních údajů. V dalších případech se uplatní naopak pouze právní úprava ochrany osobních údajů, pokud primárním účelem monitorovacího zařízení není sledování, avšak ad hoc může docházet ke zpracování osobních údajů. V řadě případů pak dochází k aplikaci jak zákoníku práce, tak i právní úpravy ochrany osobních údajů. K tomu dochází, zejména jsou-li užity prostředky moderní techniky.

Resume

The protection of personal data is a topical issue of our age, even more so nowadays with the technology constantly evolving. The aim of this thesis was to acquaint readers with the issue of personal data protection within labour relations. The thesis is primarily based on the analysis of legal regulations, especially those related to GDPR and the Labour Code. Case law, Work Party 29 statements and the Office for Personal Data Protection statements nevertheless play an important role as well. The thesis itself is split into four chapters. The first chapter focuses on the definition of basic terms, the definition of the basic terminology used and legal regulations of personal data protection. The second chapter deals with the various obligations of the employer and the rights of the employee. The third chapter describes the processing of personal data in particular stages of an employee life cycle and the last chapter is devoted to the issue of employee monitoring and surveillance, where I applied the Labour Code and Personal Data Protection legislation to diverse situations.

During the examination process of the employee monitoring and surveillance issue, I came to the conclusion that the application of the legislation is not always clear at first sight, the main reason being a rather curt legal regulation in the Labour Code. The principle of proportionality plays a particularly important role in the employment of regulations. Understanding of the specific situation and purpose of the tracking device is always essential. Nevertheless, I believe that the legal regulations of the Labour Code are sufficient as it is not possible to include all possible scenarios into them. In each case the general privacy regulation - the Civil Code - is applied. In some cases only the Labour Code regulations are then applied as well, usually when there is no processing of personal data in the monitoring process. In some cases, however, only the legal regulation of the protection of personal data applies. Nevertheless, in many cases it is both Labour code and legal regulations regarding the protection of personal data that are applied, this is particularly the case when modern technology is involved.

Seznam zdrojů

Právní předpisy a mezinárodní smlouvy

1. Evropská úmluva o ochraně lidských práv
2. Charta základních práv Evropské unie
3. Mezinárodní pakt o občanských a politických právech
4. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
5. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací
6. Smlouva o fungování Evropské unie
7. Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
8. Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat, vyhlášená pod č. 115/2001 Sb. m. s.
9. Zákon č. 262/2006 Sb., zákoník práce
10. Zákon č. 435/2004 Sb., o zaměstnanosti
11. Zákon č. 89/2012 Sb., občanský zákoník
12. Zákon č. 99/1963 Sb., občanský soudní řád
13. Zákon č. 110/2019 Sb., o zpracování osobních údajů
14. Zákon č. 40/2009 Sb., trestní zákoník

Odborná literatura a komentáře

1. BARANCOVÁ, Helena, OLŠOVSKÁ, Andrea (eds.). *Pracovné právo v digitalnej době*. Praha: Leges, 2017. ISBN 978-80-7502-259-2.
2. BARTÍK, Václav, JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi (vybrané problémy)*. 4. vydání. Praha: Wolters Kluwer ČR, a. s., 2016. ISBN 978-80-7552-141-5.

3. FIALA, Ondřej, GREPL, Jan, LICHNOVSKÝ, Ondřej. *GDPR: hmotné aspekty a procesní aspekty prakticky*. Právní praxe. Praha: C.H. Beck, 2019. ISBN 978-80-7400-762-0.
4. JANEČKOVÁ, Eva, BARTÍK, Václav. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti.* Praha: Linde, 2011. ISBN: 978-80-7201-850-5.
5. JANEČKOVÁ, Eva, BARTÍK, Václav. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3.
6. MATES, Pavel (ed.), VALOUŠEK, Martin, FIALOVÁ, Eva, LECHNER, Tomáš, HÁLOVÁ, Markéta, SIVÁK, Jakub, SOVOVÁ, Olga, BRUNA, Eduard, BRUNOVÁ, Markéta. *Ochrana osobnosti, soukromí a osobních údajů*. Praha: Leges, 2019. ISBN 978-80-7502-346-9.
7. MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. ISBN 978-80-7502-275-2.
8. MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019. ISBN: 978-80-7598-587-3.
9. MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN: 978-80-7478-139-1.
10. NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-689-7.
11. NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4.
12. NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, KOVAŘÍKOVÁ, Kristýna. *GDPR. Obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR, 2018. ISBN 978-80-7598-068-7.
13. PATTYNOVÁ, Jana, SUCHÁNKOVÁ, Lenka, ČERNÝ, Jiří. a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. Praha: Leges, 2018. ISBN 978-90-7502-288-2.

14. VALENTOVÁ, Klára, PROCHÁZKA, Jan, JANŠOVÁ, Marie, ODROBINOVÁ, Veronika, BRŮHA, Dominik a kol. *Zákoník práce.* Komentář. Praha: C. H. Beck, 2018. ISBN 978-80-7400-534-3.
15. VIDRNA, Jan, KOUDELKA, Zdeněk. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců*. Praha: C. H. Beck, 2013. ISBN 978-80-7400-453-7.
16. VLACHOVÁ, Barbora. *Zákon o zpracování osobních údajů: komentář*. V Praze: C.H. Beck, 2019. Beckovy komentáře. ISBN 978-80-7400-760-6.
17. ŽUĽOVÁ, Jana, a kol. *Spracúvanie osobních údajov zamestnanca podľa GDPR (analýza GDPR na pracovisku).* Košice: Univerzita P. J. Šafárika v Košiciach, 2018. ISBN 978-80-8152-588-9.
18. ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN: 978-80-7554-152-9.
19. ŽŮREK, Jiří. *GDPR v personalistice*. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6.

Odborné články

1. JOUZA, Ladislav. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. Bulletin advokacie, č. 6/2014.
2. KADLECOVÁ, Tereza. *Monitoring zaměstnanců*. Praktická personalistika č. 11-12/2015.
3. LIŠKUTÍN, Tomáš. *Archivace dokladů v osobních spisech zaměstnanců po skončení zaměstnání.* Praktická personalistika č. 3-4/2019, rubrika Odpovídáme na dotazy čtenářů.
4. LIŠKUTÍN, Tomáš. *Ochrana soukromí a osobních údajů uchazečů o zaměstnání (GDPR).* Praktická personalistika, č. 1-2/2018.
5. LIŠKUTÍN, Tomáš. *Ochrana soukromí a osobních údajů uchazečů o zaměstnání (GDPR) – I. část.* Praktická personalistika, č. 3-4/2018.
6. LIŠKUTÍN, Tomáš. *Ochrana soukromí a osobních údajů zaměstnanců (GDPR) – II. část.* Praktická personalistika, č. 5-6/2018.
7. MORÁVEK, Jakub. *Kontrola a sledování zaměstnanců – výklad k § 316 ZPr*. Právní rozhledy 17/2017.
8. NONNEMANN, František. *Soukromí na pracovišti*. Právní rozhledy, 7/2015.

9. RADIČOVÁ, Zuzana. *Monitoring zaměstnanců prostřednictvím GPS technologie*. Právní rozhledy, 21/2014.
10. ZEMANOVÁ ŠIMONOVÁ, Hana. *Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů*. Bulletin advokacie, č. 9/2017.
11. ŽŮREK, Jiří. *K zákonu o zpracování osobních údajů*. Praktická personalistika, č. 5-6/2019.

Judikatura

1. Rozsudek ESD ze dne 15. 7. 1964, Flaminio Costa proti E.N.E.L., věc C-6/64, EU:C:1964:66.
2. Rozsudek ESLP ze dne 12. 1. 2016, Bărbulescu proti Rumunsku, č. 61496/08.
3. Rozsudek ESLP ze dne 25. 6. 1997, Halford proti Spojenému království, č. 20605/92.
4. Rozsudek SDEU ze dne 19. 10. 2016, Patrick Breyer proti Spolkové republice Německo, věc C-582/14, EU:C:2016:779.
5. Rozsudek SDEU ze dne 6. 11. 2003, Bodil Lindqvist proti Švédsku, věc C-101/01, EU:C:2003:596.
6. Nález Ústavního soudu ČR ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17-1.
7. Nález Ústavního soudu ČR publikován pod č. 116/2008 Sb., ze dne 12. 3. 2008 ve věci návrhu na zrušení některých ustanovení zákona č. 262/2006 Sb., zákoník práce.
8. Rozsudek Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011.
9. Rozsudek Nejvyššího správního soudu ze dne 29. 7. 2009, sp. zn. 1 As 98/2008-148.
10. Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012-49.
11. Rozsudek Nejvyššího správního soudu ze dne 20. 12. 2017, sp. zn. 10 As 245/2016-41.

Stanoviska a rozhodnutí ÚOOÚ, stanoviska WP 29 a stanoviska Sboru

1. Stanovisko Evropského sboru pro ochranu osobních údajů ke zpracování osobních údajů v souvislosti s propuknutím nákazy COVID-19 ze dne 19. 3. 2020.
2. Stanovisko ÚOOÚ č. 2/2009, únor 2009 ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.
3. Stanovisko ÚOOÚ č. 3/2014, srpen 2014 k nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti.
4. Stanovisko ÚOOÚ č. 3/2009, revidované v červnu 2017 biometrická identifikace nebo autentizace zaměstnanců.
5. Stanovisko ÚOOÚ č. 5/2013, říjen 2013 pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů.
6. Stanovisko WP 29 (WP 136) č. 4/2007 ze dne 20. 6. 2007 k pojmu osobní údaje.
7. Stanovisko WP 29 (WP 249) č. 2/2017 ze dne 8. 6. 2017 ke zpracování osobních údajů na pracovišti.
8. Stanovisko WP 29 (WP 242) ze dne 13. 12. 2016 revidované a přijaté dne 5. 4. 2017 pokyny týkající se práva na přenositelnost údajů.
9. Rozhodnutí ÚOOÚ čj. UOOU-00742/13-83 ze dne 8. 3. 2013.
10. Rozhodnutí ÚOOÚ zn. INSP1-3568/12-16 ze dne 3. 1. 2013.

Elektronické zdroje

1. BOROVEC, David. Ochrana osobních údajů v personální praxi. Sborník přednášek z odborné konference Právní prostor 2018. *CODEXIS*® [online databáze]. Dostupné z https://app.codexis.cz
2. Euroskop. Listina základních práv EU. *Euroskop.cz* [online]. Vláda České republiky [cit. 10. 2. 2020]. Dostupné z: https://www.euroskop.cz/204/sekce/charta-zakladnich-prav-eu/
3. HANÁK, Jakub. Právo zaměstnavatele na narušení listovního tajemství. *Pravniprostor.cz* [online]. 2020 [cit. 3. 3. 2020]. Dostupné z

https://www.pravniprostor.cz/clanky/ustavni-pravo/pravo-zamestnavatele-na-naruseni-listovniho-tajemstvi
4. *Handbook on European data protection law* [online]. Luxembourg: Publications Office of the European Union, 2018. Dostupné z: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
5. Ke zpracování osobních údajů v rámci opatření proti šíření koronaviru: Poradna: Úřad pro ochranu osobních údajů. *Uoou.cz* [online]. [cit. 27. 3. 2020]. Dostupné z: https://www.uoou.cz/ke-zpracovani-osobnich-udaju-v-ramci-opatreni-proti-sireni-koronaviru/ds-6134/archiv=1&p1=2611
6. K rodným číslům: Úřad pro ochranu osobních údajů. *Uoou.cz* [online]. [cit. 24. 11. 2019]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5091&n=k%2Drodnym%2Dcislum
7. Monitorování zaměstnanců na pracovišti kamerovým systémem. *Suip.cz* [online]. 2014. [cit. 8. 3. 2020]. Dostupné z: http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance/monitorovani-zamestnancu-na-pracovisti-kamerovym-systemem-pridano-7-4-2014
8. POLONI, Marek. Nové trendy ve sledování zaměstnanců. *Pravniprostor.cz* [online]. 2020 [cit. 29. 2. 2020]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/nove-trendy-ve-sledovani-zamestnancu
9. Veřejný ochránce práv. Kamerové systémy a ochrana osobních údajů. *Ochrance.cz* [online]. 2012 [cit. 2. 3. 2020]. Dostupné z: https://www.ochrance.cz/ochrana-osob-omezenych-na-svobode/aktuality-z-detenci/aktuality-z-detenci-2012/kamerove-systemy-a-ochrana-osobnich-udaju/
10. Zaměstnavatelé: Úřad pro ochranu osobních údajů. *Uoou.cz* [online]. [cit. 6. 3. 2020] Dostupné z: https://www.uoou.cz/zamestnavatele/ds-5057

Ostatní zdroje

1. 138/0 vládní návrh na vydání zákona o zpracování osobních údajů

2. 16/0 senátní návrh zákona o svobodném přístupu k informacím a o změně dalších zákonů
3. *Provozování kamerových systémů*: *metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů*. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2012. ISBN 978-80-210-6017-3.
4. Všeobecná deklarace lidských práv