

Západočeská univerzita v Plzni

Fakulta právnická

Katedra pracovního práva a práva sociálního zabezpečení

DIPLOMOVÁ PRÁCE

Ochrana osobních údajů v pracovněprávních vztazích

Bc. Marie Kudová

Plzeň 2024

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Bc. Marie KUDOVÁ**
Osobní číslo: **R19M0208P**
Studijní program: **M0421A220004 Právo a právní věda**
Téma práce: **Ochrana osobních údajů v pracovněprávních vztazích**
Zadávající katedra: **Katedra pracovního práva a práva sociálního zabezpečení**

Zásady pro vypracování

1. Úvod
2. Základní pojmy
3. Prameny práva a zásady zpracování osobních údajů
4. Práva a povinnosti zaměstnance a zaměstnavatele
5. Ochrana údajů v jednotlivých fázích pracovního poměru
6. Monitoring zaměstnanců
7. Závěr

Rozsah diplomové práce:
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

- viz příloha

Vedoucí diplomové práce: **Doc. JUDr. Jakub Morávek, Ph.D.**
Katedra pracovního práva a práva sociálního
zabezpečení

Datum zadání diplomové práce: **16. ledna 2023**
Termín odevzdání diplomové práce: **31. března 2024**



JUDr. et PhDr. Stanislav Balík, Ph.D.
děkan



Doc. JUDr. Jakub Morávek, Ph.D.
vedoucí katedry

V Plzni dne 5. září 2023

Prohlášení

Prohlašuji, že jsem diplomovou práci na téma „*Ochrana osobních údajů v pracovněprávních vztazích*“ zpracovala samostatně a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala způsobem pro vědeckou práci obvyklým.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 176 763 znaků včetně mezer.

V Plzni dne:

podpis studenta:

Obsah

Seznam použitých zkratk	7
Úvod	8
1. Základní pojmy	10
1.1. Právo na soukromí	10
1.1.1. Soukromí v pracovním prostředí	13
1.2. Pojem osobní údaje	14
1.3. Zvláštní osobní údaje	16
1.3.1. Problematika rodných čísel	17
1.4. Zpracování osobních údajů	18
1.4.1. Zákonnost zpracování	19
1.5. Správce a zpracovatel	21
2. Prameny práva	23
2.1. Vývoj ochrany osobních údajů	23
2.1.1. Všeobecná deklarace lidských práv	23
2.1.2. Evropská úmluva o ochraně lidských práv a svobod	24
2.1.3. Mezinárodní pakty	25
2.1.4. Směrnice Rady OECD	26
2.2. Unijní právní úprava	28
2.2.1. Směrnice 95/46/ES	28
2.2.2. Obecné nařízení o ochraně osobních údajů	29
2.3. Vnitrostátní právní úprava	30
2.4. Zásady zpracování osobních údajů	32
2.4.1. Zásada zákonnosti	33
2.4.2. Zásada korektnosti a transparentnosti	34
2.4.3. Zásada integrity a důvěrnosti	36
2.4.4. Zásada přesnosti	36
2.4.5. Zásada minimalizace údajů	37
2.4.6. Zásada omezení uložení	38
3. Práva a povinnosti	39
3.1. Povinnosti zaměstnavatele	39
3.1.1. Zpracování na základě souhlasu	40
3.1.2. Informační povinnost	42
3.1.3. Povinnost zabezpečit údaje	43
3.1.4. Ohlašovací povinnost	44
3.2. Práva subjektu	45

3.2.1.	Právo na přístup k osobním údajům.....	46
3.2.2.	Právo na opravu.....	46
3.2.3.	Právo na výmaz.....	47
3.2.4.	Právo na omezení zpracování.....	47
3.2.5.	Právo na přenositelnost údajů.....	48
3.2.6.	Právo vznést námitku.....	48
3.2.7.	Právo nebýt předmětem rozhodování založeného na automatizovaném zpracování osobních údajů.....	49
4.	Ochrana osobních údajů v jednotlivých fázích pracovního poměru.....	50
4.1.	Ochrana před vznikem pracovního poměru.....	50
4.1.1.	Uvedení nepravdivých informací uchazečem.....	52
4.1.2.	LinkedIn, jako prostředek pro výběr uchazečů.....	52
4.2.	Ochrana při výkonu práce.....	54
4.2.1.	Osobní spis zaměstnance.....	57
4.2.2.	Požíování kopií dokladů.....	59
4.2.3.	Uveřejňování fotografií zaměstnanců.....	59
4.3.	Skončení pracovního poměru.....	61
5.	Monitoring zaměstnanců.....	64
5.1.	Kamery na pracovišti.....	67
5.1.1.	Použití falešných kamer.....	69
5.2.	Elektronická pošta.....	69
5.3.	Služební telefony a počítače.....	70
5.4.	GPS.....	72
5.5.	Sledování aktivit zaměstnanců na internetu.....	73
5.6.	Homeoffice.....	76
Závěr.....		78
Resume.....		80
Klíčová slova.....		80
Keywords.....		80
Zdroje.....		81

Seznam použitých zkratk

EÚLP	Evropská úmluva o ochraně lidských práv a základních svobod
GDPR	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 (obecné nařízení o ochraně osobních údajů)
Směrnice	směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
Úmluva (Úmluva č. 108)	Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. 1. 1981.
ÚOOÚ	Úřad pro ochranu osobních údajů
WP29	Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená směrnicí 95/46/ES podle článku 29. Nezávislý evropský poradní orgán na ochranu dat a soukromí, který se s účinností Nařízení změnil na Evropský sbor pro ochranu osobních údajů.
ZOOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
ZP	Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
ZZOÚ	Zákon č. 110/2019 Sb., o zpracování osobních údajů

Úvod

Ochrana osobních údajů představuje poměrně mladou právní disciplínu, která se systematicky vyčlenila z práva na soukromí v průběhu 80. let a v podstatě vždy reagovala na rozvíjející se moderní technologie, ať už to bylo při vzniku směrnice 95/46/ES anebo novějším nařízením Evropského parlamentu a Rady EU 2016/679, známého také pod názvem GDPR. Oba dokumenty ve své době reagovaly na potřebu vyvíjející se společnosti i rizika, která sebou nové technologie ve vztahu k ochraně osobních údajů přinášely.

Žijeme v době, kdy je svět čím dál tím více digitalizován, propojován a přenos dat i jejich ochrana je každodenní rutinou. I z tohoto důvodu je ochrana osobních údajů stále se rozvíjející oblastí a aktuálním tématem, která se dotýká každého člověka od narození (případně nascitura) až do smrti.

Práce a její výkon tvoří podstatnou roli v životě téměř každého jedince. Většina lidí v určité fázi svého života hledá, vykonává anebo ukončuje pracovní poměr a málokdo ví, jaké osobní údaje od nich mohou být v které fázi vyžadovány, či jaké mají práva ve vztahu ke svým poskytnutým údajům. Právo ochrany osobních údajů je oblastí, která obsahuje širokou řadu neurčitých právních pojmů (koneckonců cílem je ochrana soukromí, což je sám o sobě těžko definovatelný abstraktní pojem), které se interpretují v duchu určitých zásad vymezených, jak mezinárodním právem, tak unijní agendou, což prohlubuje složitost tématu pro laickou veřejnost.

Dané téma je velice široké a lze na něj nahlížet z mnoha úhlů. Již samotný vývoj ochrany osobních údajů je velmi zajímavým a obsáhlým tématem, který by zaplnil mnoho stran. Cílem práce je tedy přiblížení ochrany osobních údajů v souvislosti s jednotlivými fázemi pracovního poměru a vystihnout postavení obou stran v rámci pracovního procesu a provázanost jejich vzájemných práv a povinností, které vůči ochraně osobních údajů mají.

Diplomová práce je systematicky členěna do pěti hlavních kapitol. První kapitola se věnuje základním pojmům, včetně pojmu soukromí, ze kterého se postupně vyčlenilo právo na ochranu osobních údajů a které by se dalo označit za ústřední pojem této práce, neboť je to soukromí, co chceme chránit a kvůli kterému vznikla celá nová právní oblast.

Druhá kapitola je zaměřena na vývoj ochrany osobních údajů, popsany skrz podstatné mezinárodní dokumenty a další dokumenty přijaté na unijní úrovni.

Pozornost je věnována zejména směrnici 95/46/ES a obecnému nařízení GDPR, které představuje právní rámec ochrany osobních údajů nejen v prostoru evropské unie, ale také v rámci vnitrostátní úpravy, kde je podstatným hlavně zákon o zpracování osobních údajů. Obsahem této kapitoly jsou i zásady zpracování osobních údajů, které představují základní principy, kterými je ovládáno každé zpracování a společně s třetí kapitolou přibližují právní úpravu obsaženou v GDPR a upozorňují na provázané postavení obou stran skrz. Jednou z podstatných povinností zaměstnavatele jako správce je existence právního titulu pro zpracování údajů. Právní tituly jsou definovány v první kapitole, ale v rámci práv a povinností obou stran se autorka rozhodla zaměřit na zpracování na základě souhlasu a oprávněného zájmu zaměstnavatele, které vnímá, jako nejvíce problematické.

Čtvrtá kapitola je zaměřena na jednotlivé fáze pracovního procesu a nakládání s osobními údaji, kdy se autorka snažila zahrnout do práce i určité modelové situace, jako je zpracování údajů s využitím umělé inteligence při náboru uchazečů anebo kopie dokladů při po podpisu pracovní smlouvy.

V poslední kapitole se autorka věnuje kontrole zaměstnanců a monitoringu v rozličných situacích, kdy se na zaměstnavatele klade značná odpovědnost, neboť se zde dostávají do kolize ústavně zaručená práva obou stran pracovního poměru.

1. Základní pojmy

V každé právní oblasti je vhodné si na začátek vymezit základní pojmy. V rámci ochrany osobních údajů existují 4 základní pojmy, které definovala již Úmluva č. 108 a daly by se tak označit jako nejstarší. Jednalo se o pojmy: osobní údaj, zpracování, automatizovaný datový soubor (automatizace) a správce osobních údajů. Kromě definic v čl. 2 obsahovala Úmluva ve svých dalších ustanovení i definici citlivé údaje, které stejně, jako dnešní úprava vymezovala v rámci taxativního seznamu a zakazovala automatizované zpracování, pokud vnitrostátní úprava nestanoví jinak. Pojem zpracovatel osobních údajů se objevil až později, a to v reakci na právní úpravu EU vycházející z nařízení GDPR 2016/679, které samo převzalo většinu definic ze Směrnice 95/46/ES.

Čtveřice základních pojmů zůstala ve svém jádru téměř neměnná, ale s postupem doby se rozšiřovala množina základních pojmů, zejména v souvislosti s modernizací technologií a většímu využívání automatizovaných postupů. V současné době jsou základní pojmy komplexně upraveny v GDPR, a to především v příslušných recitálech a čl. 4, který je i příhodně nazván „*definice*“. Vnitrostátní právní úprava, představovaná především ZZOU neobsahuje vlastní seznam definic základních pojmů, jako jeho předchůdce ZOOÚ, který převzal seznam základních pojmů i jejich definice ze směrnice 95/46/ES.

Kromě těchto zákonů, se můžeme s pojmy souvisejícími s ochranou osobních údajů setkat i v dalších právních předpisech, jako je například zákon o evidenci obyvatel, upravující používání rodných čísel.

1.1. Právo na soukromí

Ještě, než začnu s rozebráním jednotlivých základních pojmů, chtěla bych se věnovat právu na soukromí, které bývá vnímáno, jako předchůdce práva na ochranu osobních údajů a až teprve v průběhu času a zejména díky nastoupení moderních technologií došlo k rozlišení práva na soukromí a práva na ochranu osobních údajů, přičemž dodnes jsou obě právní oblasti úzce spjaty.¹

Spojení těchto dvou právních odvětví můžeme nalézt v samotných předpisech upravujících ochranu osobních údajů, tak v judikatuře.

¹ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s. 23.

Úmluva č. 108 v čl. 1 zmiňuje: „Účelem Úmluvy je zaručit každé osobě úctu k jejím úctu k jejím právům a zejména k právu na soukromý život se zřetelem k automatizovanému zpracování osobních údajů“.²

Směrnice 95/46/ES, která je pokračovatelem Úmluvy a značnou část základních práv, zásad a povinností z ní převzala, stanovuje v bodu. 2, že při zpracování osobních údajů musí být dodržovány základní svobody a práva, zejména právo na soukromí. Zatímco z Úmluvy ještě není patrné oddělení právních oblastí, ve směrnici již můžeme vnímat, že jsou obě právní odvětví brána, jako samostatná, přestože v podstatě jedno nemůže být bez druhého a panuje mezi nimi až rodinný vztah, neboť nemůžeme zajistit dostatečnou ochranu soukromí člověka, bez toho, aniž bychom chránili jeho osobní údaje.³ Održení ochrany osobních údajů od práva na soukromí můžeme mimo jiné podložit i tím, že se jeho samostatná úprava neodkazující se na právo na soukromí objevuje i mezi základními právy Listiny základních práv EU a v čl. 16 Smlouvy o fungování EU a koneckonců v nařízení GDPR už o právu na soukromí nenajdeme ani zmínku.⁴

Definovat a plně vystihnout samotný pojem soukromí není vůbec jednoduché a může se to zdát nemožné. Americká profesorka Judith Jarvis Thompson uvedla, že: „*tou nejpozoruhodnější věcí na právu soukromí, je to, že nikdo nemá zřejmou představu o tom, co to vlastně je*“⁵ a celkově se k pojmu soukromí stavěla velmi skepticky s tím, že není ani tak podstatné specifikovat samotný pojem, ale je vhodné se spíše soustředit na primární práva s jeho ochranou spojená.

Mnoho autorů, jako Roger Clark, Louise Brandeise nebo Alan Westin, rozdělovali soukromí do více kategorií, ve snaze vystihnout jeho komplexní povahu, a přestože počet kategorií nebyl konstantní, můžeme vysledovat, že se za soukromí v podstatě považuje veškerý intimní prostor člověka a místa, kde se zdržuje a očekává, že bude sám a nerušen.⁶ Myšlenka, že soukromí vlastně znamená

² MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita, 2020. ISBN 978-80-210-9736-0. str. 27 a 29

³ MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s. 22-25

⁴ tamtéž

⁵ THOMSON, Judith Jarvis. *The Right to Privacy*. *Philosophy & Public Affairs*. 1975, 4(4), 295–314. ISSN 0048- 3915. s. 295

⁶ MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita, 2020. ISBN 978-80-210-9736-0. str. 27 a 29

určitou zónu klidu, kde je člověk ponechán sobě samému představili poprvé bostonští advokáti Samuel Warren a Louise Brandeise ve slavném článku z roku 1890 „*The Right to Privacy*“, který je považován za první text koncipující právo na soukromí. Už v tomto článku upozorňovali na potřebu činit další kroky v ochraně člověka, vzhledem k pokrokům v informačních a komunikačních technologiích.⁷ Problematiku definice soukromí ještě znesnadňuje fakt, že se jedná o značně dynamický pojem, který se mění s vývojem času i s vývojem lidské společnosti. V dnešní době a s rozvojem moderních technologií a široké přítomnosti online prostředí, je ochrana soukromí a osobních údajů, ne že potřebnější, neboť potřebná byla vždy, nicméně spíše širší, a to hlavně kvůli množství možných uniklých dat, sledování aktivit a potencionálního většího zásahu do soukromí.⁸

Když se přesunu v čase, do doby ne tak nedávné, tak definici soukromí, respektive soukromého života se vyhnul i Evropský soud pro lidská práva, který v rozsudku *Niemitz proti Německu* z roku 1992 uvedl, že není možné a ani nezbytné podat vyčerpávající definici pojmu soukromý život, ale zároveň stanovil, že se soukromí netýká pouze vnitřního kruhu jedince, jak se mnozí domnívali, ale i pracoviště, neboť právě na pracovišti dochází k rozvíjení vztahů a sociálních interakcí.⁹ V souladu s tímto rozhodnutím jednal i Ústavní soud ČR v nálezu ze dne 1. 3. 2000 sp. zn. II. ÚS 517/99, ve kterém „*zdůrazňuje myšlenku, že respektování soukromého života musí do určité míry zahrnovat právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi*“.¹⁰

Samotný pojem soukromí je hodně spjat s vnímáním jednotlivců, kdy se má jednat o místo, kde má jedinec možnost chovat se svobodomyšlně, bez naplňování určitých sociálních rolí a mít právo na určitou míru diskretnosti, bez větší míry ostražitosti. Z toho vyplývá, že se může jednat v podstatě o jakékoliv místo, které naplní v jednotlivci tato očekávání a pracoviště by takovým místem být mělo.¹¹

Novodobé definice soukromí, jsou sice stále široké a variabilní, nicméně víceméně upozorňují na to, že koncept soukromí zasahuje, jak do fyzické, tak

⁷ ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3.

⁸ MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s. 22-25

⁹ Rozsudek ESLP ve věci *Niemietz v. Německo* ze dne 16. 12. 1992, stížnost č. 13710/88

¹⁰ Nález Ústavního soudu ČR ze dne 1. 3. 2000 sp. zn. II. ÚS 517/99.

¹¹ ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3.

mentální roviny jedince a ani zdaleka se netýká jen jeho vlastní osoby a nejbližšího prostoru (jako je obydlí), ale součástí soukromého života je i právo na vytváření a rozvíjení vztahů.¹²

Soukromí je chráněno na národní, tak nadnárodní úrovni, a to v právních předpisech nejvyšší síly. V českém právním řádu ho najdeme ve vícero člancích Listiny základních práv a svobod, kdy výčet nelze považovat za konečný. Konkrétně se jedná o čl. 7 odst. 1 nedotknutelnost osoby a jejího soukromí obecně, dále čl. 10 ochrana před neoprávněnými zásahy do soukromého a rodinného života, čl. 12 ochrana obydlí a čl. 13 ochrana listovního tajemství.¹³ Kromě LZPS najdeme související právní normy i v občanském zákoníku, zákoníku práce.

1.1.1. Soukromí v pracovním prostředí

Z výše zmíněného rozsudku *Niemietz vs Německo*, jasně vyplývá, že i pracoviště je prostorem, kde musí být chráněno soukromí zaměstnance. Zaměstnanci mají legitimní nároky, na bezpečné pracovní prostředí, nicméně nemůžeme tento nárok omezovat pouze na podmínky, které by mohly ohrozit tělesnou stránku, jako nepříznivá teplota, hluk špatné světlo, prašnost atd., ale podstatné jsou i správně nastavené limity ve vztahu k možným zásahům do soukromí.¹⁴

V rozhodovací praxi ESLP zaujal postoj, že nelze zcela oddělit pracovní a rodinný život, neboť právě v rámci pracovního prostředí vznikají důležité sociální interakce a navazování vztahů, které taktéž spadají pod ochranu soukromí. Mnoho jedinců se vyjadřuje, že je pro ně pracovní kolektiv velmi podstatný z hlediska sociálních vazeb. V rámci zaměstnání mohou najít i životní partnery a pracovní prostor může působit, jako druhý domov, kde by měli pociťovat stejnou míru bezpečí a klidu, jako v případě obydlí, tudíž by i zde měla být stejná míra ochrany.¹⁵

Ochranu soukromí na pracovišti nemůžeme pevně spojit s jedním konkrétním místem, jako je např. kancelář, už kvůli možnosti pracovních cest zaměstnanců, sdílených míst anebo práce z domova. Z toho vyplývá, že ani míra

¹² Úřad pro ochranu osobních údajů. Stanovisko č. 6/2009. [online] 2009 [cit. 2019-12-20]. Dostupné z: https://www.uoou.cz/files/stanovisko_2009_6.pdf

¹³ Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod.

¹⁴ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovníprávní vztahy. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s. 22-25

¹⁵ tamtéž

ochrany soukromí nebude na všech pracovních místech stejná, ale bude určována podle prostor, kde se zaměstnanec nachází, časovým úsekem, kdy se v ní nachází a jeho vztahem k danému místu. Podstatným faktem je také legitimní očekávání, anebo také rozumné očekávání soukromí, se kterým se setkáváme velmi často v judikatuře ESLP. Tento pojem odkazuje na informovanost zaměstnanců ohledně toho, jak jsou při své práci sledováni, kdy dostatečná informovanost napomáhá vybudovat dlouhodobé kvalitní pouto mezi zaměstnavatelem a zaměstnancem.¹⁶

1.2. Pojem osobní údaje

Vzhledem k tomu, že je celá právní oblast nazvána jako ochrana osobních údajů, je důležité si pojem osobní údaj správně definovat, neboť GDPR se vztahuje pouze na zpracovávání informací, které lze za osobní údaje označit a jen těchto údajů se týká ochrana ze strany GDPR či vnitrostátních předpisů.

GDPR definuje osobní údaje jako: „*veškeré informace, které se týkají identifikované nebo identifikovatelné žijící osoby*“.¹⁷

Jako první se zaměříme na to, co jsou „*veškeré informace*“. Ze samotné textace, je zřejmý úmysl zákonodárce neklást hranice pojmu osobní údaj a vykládat ho nikoliv restriktivně, nýbrž extenzivně. Podle pokynů WP29 si pod pojmem veškeré informace můžeme představit všechny druhy tvrzení o osobě bez ohledu na jejich skutečnou výpovědní hodnotu. Může se tedy jednat o informace objektivní, subjektivní, pravdivé či prokázané a nezáleží ani na formě v jaké jsou vyjádřeny. Můžeme se tak jednat i o hodnocení nebo názory, poukazující na charakterní znaky člověka (např. zda je někdo důvěryhodný nebo jaké má pracovní zkušenosti).¹⁸

Aby se informace stala osobním údajem a byla tkz. *identifikátorem*, musí zde být konkrétní vazba na určitého jedince, kterého díky nim můžeme plně rozpoznat, tudíž identifikovat v rámci širší skupiny lidí. Tyto identifikátory mohou být přímé nebo nepřímé. Za přímé se z pravidla považují informace ohledně jména, příjmení, adresy a datumu narození, kdy jejich kombinací může dojít k poměrně rychlému a snadnému rozpoznání osoby. I tak, je nicméně musíme vždy vnímat

¹⁶ ŠTEFKO, Martin. Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochraně lidských práv a základních svobod. Jurisprudence. 2012, 21(7-8), 17-21. ISSN 1802-3843.

¹⁷ Recitál č. 26 GDPR a čl. 4 odst. 1 GDPR.

¹⁸ Stanovisko č. 4/2007 K pojmu osobní údaje. WP 136. Pracovní skupina pro ochranu údajů zřízená podle článku 29 [online]. Evropská komise, © 2007, s. 6–7 [cit. 10. 3. 2024].

v kontextu situací.¹⁹ Jméno a příjmení Jan Novák by se mohlo zdát jako dostatečnou informací k určení osoby, nicméně i v rámci velké firmy, se může stát, že pracujících Janů Nováků v ní bude více, tudíž na základě této informace není možné konkrétní osobu identifikovat a o osobní údaj se jednat nebude. Pokud by však došlo ke spojení tohoto přímého identifikátoru s nepřímou informací např. Jan Novák, pracující na oddělení marketingu, poté by v souhrnu tyto informace mohly být dostačené k určení konkrétní osoby a jednalo by se o osobní údaje. Stejný princip se uplatní i v případě pracovní emailové adresy, za použití stejného jména jan.novak@....na běžně používaném internetovém serveru je dostatečně neurčitá, aby se o osobní údaj nejednalo. Ovšem pokud e-mailová adresa bude mít znění jan.novak@jmenofirmy.cz už osobním údajem je, neboť název firmy za jménem je dostatečným nepřímým identifikátorem k určení osoby.²⁰

Nepřímo můžeme osobu identifikovat pomocí telefonního čísla, čísla cestovního pasu, anebo kombinací dalších jedinečných znaků člověka (jako je vzhled, vzdělání, styl chůze a další přidaná hodnocení), které ho umožní rozeznat v rámci skupiny. Nepřímé identifikátory často potřebují přítomnost dalšího identifikátoru, aby dopomohly k bližšímu určení osoby, ale i jejich dostatečnou kombinací může dojít k rozeznání. Jedná se o situace, kdy již víme, o jakou konkrétní osobu se jedná a shromažďujeme o ní další informace.²¹

Osobě, k níž se dané osobní údaje vztahují, pak říkáme *subjekt osobních údajů*. Subjektem je osoba, kterou lze přímo nebo nepřímo identifikovat, s odkazem na nějaký identifikátor, kterým může být prakticky cokoli.²² Subjektem nemůže být zemřelá osoba, ani právnické osoby, ledaže by bylo postavení jedince v rámci organizační struktury právnické osoby dostatečné na jeho identifikaci (např. člen kontrolní komise anebo ředitel společnosti). Poté by se jednalo o osobní údaje, které již ochranu podle předpisů na ochranu osobních údajů požívají.²³ Sporné otázky se v minulosti vyskytly v souvislosti s ochranou osobních údajů fyzických

¹⁹ FIALA, O. Kapitola I. Obecný úvod do GDPR. In: FIALA, GREPL, LICHNOVSKÝ 2019 op. Cit. Str16-18

²⁰ Mihulková, J.; Kornel, M. Co je, co není a co bude osobní údaj podle GDPR, 10. 2. 2018. Frank Bold Advokáti. (citováno dne 10. 3. 2024). Dostupné z: <https://www.fbadvokati.cz/cs/clanky/541-co-je-co-neni-a-co-bude-osobni-udaj-podle-gdpr>

²¹ Rozsudek městského soudu v Praze sp.z.11 ca 433/2008 Sb. a srov. Recitál č. 26 GDPR.

²² MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s. 109-120

²³ tamtéž

podnikajících osob, kvůli blízké provázanosti jejich soukromého a pracovního života. Přestože jsou v případě podnikajících osob mnohé údaje veřejně dostupné, došel ÚOOÚ ve svém stanovisku č. 3/2011 k názoru, že statut osobních údajů by měly mít minimálně informace související s živnostenskou činností osob a jejich zpracování by mělo probíhat v souladu ochrany osobních údajů. Své rozhodnutí podložil stanoviskem WP 29 č. 4/2007, kdy jednou z informací (nepřímým identifikátorem) je i ekonomická identita jednotlivce.²⁴ Toto stanovisko zaujalo opačný názor, než nález Ústavního soudu České republiky č. 299/2004 Sb., který údaje o činnosti podnikající fyzické osoby za osobní údaje nepovažoval, právě kvůli veřejnému zveřejňování a snadnému dohledání v příslušných rejstřících. Takovýto postup, však správnému orgánu nepřisluší, mimo jiné proto, že podrývá autoritu Ústavního soudu a právní jistotu adresátů vůči němu. Situaci vyjasnilo GDPR, které ochranu informacím ohledně podnikatelských činností přiznává, ale upozorňuje na jejich malou rizikovost.²⁵

Osobní údaje, které byly zbaveny informačních hodnot takovým způsobem, že příslušná osoba z nich, jichž není identifikovatelné, osobními údaji nejsou. Jedná se zejména o anonymizované údaje nebo obecné informace, jako je například emailová adresa firmy, odkazující na personálního oddělení, bez uvedení konkrétního jména.

1.3. Zvláštní osobní údaje

Osobních údajů může být nepřeberné množství. Nicméně bylo nutné vyčlenit speciální podskupinu těch, které potřebují zvýšenou ochranu pro svou citlivou povahu z hlediska základních práv a svobod jedinců a většího potenciálu poškození subjektu údajů.²⁶ V ZOOÚ byly tyto údaje označovány jako citlivé, což je termín, který najdeme i v recitál č. 10 GDPR (kde jsou oba pojmy, jak zvláštní, tak citlivé údaje uvedeny jako synonyma), ale jako legislativní zkratku je dále GDPR nevyužívá a definice v čl. 9 GDPR používá slovní spojení zvláštní osobní údaje, které budu využívat i v rámci této práce.²⁷ Co se týče platné vnitrostátní

²⁴ Stanovisko č. 3/2011: Ochrana osobních údajů podnikajících fyzických osob. Úřad pro ochranu osobních údajů [online] a § 4 písm. a) ZOOÚ

²⁵ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s. 109-120 a nález Ústavního soudu ze dne 9. 3. 2002 č. 299/2004 Sb.

²⁶ Recitál č. 51 GDPR

²⁷ Recitál č. 10 GDPR

úpravy, je vhodné zmínit, že současné znění zákona ZOZÚ se věnuje zvláštním údajům v přechodném ustanovení § 66 odst. 6 a definice je shodná s tou v čl. 9 GDPR, který obsahuje výčet zvláštních údajů.²⁸

Jedná se o údaje:

- vypovídající o rasovém anebo etnickém původu;
- prozrazující náboženské vyznání, politické názory anebo filozofické přesvědčení či členství v odborech;
- genetické a biometrické údaje, pořízení za účelem jedinečné identifikace osoby;
- údaje o zdravotním stavu a sexuální orientaci.

Kromě taxativního seznamu uvedeného v GDPR mají státy v rámci své vnitrostátní legislativy možnost specifikovat další údaje, které zaměstnavatel nesmí požadovat. Zvláštním údajům se věnuje i zákoník práce, který v §316 odst. 4 zakazuje další informace nad rámec GDPR, které zaměstnavatel nesmí požadovat, jedná se o informace zejména o rodinných a majetkových poměrech.

1.3.1. Problematika rodných čísel

Do zvláštních údajů překvapivě nepatří rodné číslo, které je považováno optikou GDPR za obyčejný osobní údaj, přestože z něho můžeme vyčíst mnoho dalších informací, jako je datum narození, pohlaví nebo věk. Rodné číslo, je tak unikátním identifikátorem a zákon o evidenci obyvatel v § 13 odst. 1 na rozdíl od GDPR do jisté míry omezuje jeho užívání. Z praktického hlediska to tedy znamená, že právní důvody zpracování rodných čísel zaměstnanců nebudeme hledat v GDPR, ale ve vnitrostátní úpravě. Ustanovení § 13 odst. 1 písm. c) stanovuje, že rodná čísla lze využívat jen, jde-li o činnost ministerstev a jiných správních orgánů pověřených výkonem státní správy, pokud tak stanoví zvláštní zákon anebo pokud jeho nositel dá souhlas. Mohlo by se tedy zdát, že ke zpracování rodných čísel bude vždy potřeba souhlasu, tak tomu ale není. Je nutné ještě připomenout, že rodné číslo nemusí být uváděno v životopise, ani na pohovoru a nemusí být uvedeno ani na pracovní smlouvě. Nicméně po uzavření pracovní smlouvy vznikají zaměstnavateli zákonné oznamovací povinnosti vůči zdravotním pojišťovnám a České správě

²⁸ ZAHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 163

sociálního zabezpečení, kde bude rodné číslo vyžadováno. Souhlas zaměstnance tak prakticky není potřeba.²⁹

Po schválení novely zákona č. 269/2011 Sb. o občanských průkazech, nemá být rodné číslo uváděno v občanských průkazech, i přesto, že doposud bylo běžně užívaným identifikátorem fyzických osob při uzavírání smluv, mimo jiné i těch pracovních.³⁰ Důvodem této novelizace byly obavy o zneužívání rodných číslem, kdy jejich uvádění v občanských průkazech představuje závažná rizika. K nezbytnosti ochrany rodného čísla se opakovaně vyjadřoval také ÚOOÚ, který kritizoval úplné zrušení rodných čísel, bez toho, aniž by byla zvolena adekvátní náhrada, nehledě na odklady termínů, od kdy tedy nebudeme rodná čísla smět používat (datum po posledním odkladu bylo stanoveno na konec roku 2023), což podřývalo právní jistotu adresátů.³¹ Z mého pohledu je zvláštní, že i přes dlouhotrvající diskuze, směřující k omezování rodných čísel a poukazování na jejich rizikovost, je rodné číslo stále jen běžným údajem, který nepodléhá výjimkám zvláštního zpracování údajů.³²

1.4. Zpracování osobních údajů

Definice zpracování osobních údajů, jak ji najdeme v čl. 4 odst. 2 GDPR je velmi široká a za zpracování považuje jakékoliv operace, které jsou s osobními údaji anebo se souborem osobních údajů prováděny, ať už s pomocí či bez pomoci automatizovaných postupů. Automatizovaného postup je činěn především prostředky výpočetní techniky, a to víceméně nezávisle na lidské vůli, jako příklad můžeme uvést kamerové systémy, kdy nahrávání dat a pořizování záznamů se děje automaticky anebo uložení dat na CD případně do online prostředí pomocí cloudu. Neautomatizované zpracování by poté odpovídalo zpracování manuálnímu, v listinné podobě, například při přinesení životopisu uchazeče o zaměstnání, kdy tento bude uložen do evidence. Evidencí se rozumí netechnická zařízení, do kterých jsou data ručně zadávána a která následně slouží k dalšímu zpracování údajů.

²⁹ Zákon o veřejném zdravotním pojištění a zákona o nemocenském pojištění

³⁰ Nakládání s rodnými čísly v kontextu GDPR | epravo.cz. (n.d.). EPRAVO.CZ. Dostupné z: <https://www.epravo.cz/top/clanky/nakladani-s-rodny-mi-cisly-v-kontextu-gdpr-108254.html>

³¹ Rozumné právo. (2021, April 16). Konec rodných čísel v občanských průkazech. Právní prostor. Dostupné z: <https://www.pravniprostor.cz/clanky/ostatni-pravo/konec-rodnych-cisel-v-obcanskych-prukazech>

³² Řepka, M. (2023, November 27). Úřad pro ochranu osobních údajů. Titulní stránka | Úřad pro ochranu osobních údajů. <https://uouu.gov.cz/novinky/vse/rodna-cisla-by-v-obcanskych-prukazech-nemela-byt-uvadena>

Demonstrativní výčet zpracování osobních údajů dle GDPR:

- shromáždění, zaznamenání a uspořádání osobních údajů
- strukturování a uložení osobních údajů
- přizpůsobení nebo pozměnění osobních údajů
- vyhledání, nahlédnutí, použití osobních údajů
- jakékoliv jiné zpřístupnění, seřazení či zkombinování osobních údajů
- omezení, výmaz či zničení osobních údajů³³

Ochrana údajů v rámci GDPR se nevztahuje na nahodilé shromažďování osobních údajů a jak bylo řečeno výše, nevztahuje se ani na informace, které osobními údaji nejsou.³⁴ Příkladem nahodilého shromáždění, může být obdržení mylné emailové zprávy, určené jinému příjemci, kdy obsahem zprávy budou osobní údaje zaměstnanců. Pokud bude email po doručení špatnému příjemci odstraněn a nadále nebude s údaji zacházeno, nebude se na takové jednání GDPR vztahovat. Dalším zpracování nebude ani předání osobních údajů, pokud bude zřejmé, komu původní email směřoval a osoba, které byl mylně doručen jej odešle správnému příjemci.³⁵

1.4.1. Zákonnost zpracování

Aby bylo zpracování údajů legální, musí být udán minimálně jeden právní důvod, pro který mají být zpracovány. Důvody k zpracování běžných osobním údajům najdeme v čl. 6 odst. 1 GDPR

- a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;*
- b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;*
- c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;*
- d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*

³³ Recitál č. 15 GDPR

³⁴ ŽŮREK, Jiří. GDPR v personalistice. Práce, mzdy, pojištění. Olomouc: ANAG, [2019]. ISBN 978-80-7554-210-6.

³⁵ Nahodilé zpracování osobních údajů. (n.d.). Portál daňových poradců a účetních profesionálů (cit. 11. 3. 2024). Dostupné z: <https://www.dauc.cz/clanky/5655/nahodile-zpracovani-osobnich-udaju>

- e) *zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce*
- f) *zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.*³⁶

Pro kategorii zvláštních osobních údajů je jejich zpracování připuštěno v čl. 9 odst. 2 GDPR a spíše, než o právních důvodech se hovoří o výjimkách, za kterých mohou být zpracovány. Ve vztahu k čl. 6 odst. 1 GDPR můžeme vyzorovat, že výjimky mají přísnější znění.³⁷ U běžných údajů dle písm. a) postačí souhlas subjektu, v případě zvláštních údajů se zpracování připouští po udělení výslovného souhlasu pro konkrétní účel nebo účely. Obdobný princip najdeme v případě zpracování údajů ve veřejném zájmu, kdy zvláštní údaje mohou být zpracovány pouze ve „významném“ veřejném zájmu.³⁸ O veřejném zájmu se zmiňuje i recitál č. 10, který poukazuje na cíl zajistit soudržnou a vysokou úroveň ochrany fyzických osob s tím, že napříč státy unie mají být dodržovány tyto vysoké standardy ochrany, nicméně v případě veřejného zájmu, kdy každý členský stát ho může vnímat lehce odlišně, mají státy pravomoc zavést vnitrostátní předpisy, kde budou konkretizovat uplatňování pravidel GDPR. Významný veřejný zájem tak může v každém členském státu být vnímán s mírnými odlišnostmi.³⁹

Pokud v případě běžného údaje není subjekt způsobilý k tomu dát souhlas, můžeme k jejich zpracování přistoupit v případě, že se jedná o informace, které sám zveřejňuje, anebo pokud je to nezbytné pro plnění smlouvy, jak uvádí čl. 6 písm. b). V případě zvláštních údajů toto udělat nemůžeme, kromě výjimky, kdy by mělo dojít k plnění povinností v oblasti pracovního práva nebo sociálního zabezpečení a v případně zpracování nezbytného pro určení, výkon nebo obhajobu právních nároků dle čl. 9 odst. 2 písm. f) GDPR.⁴⁰

Z výše uvedeného, je zřejmé, že v případě zvláštních údajů se nejedná o výjimky, které by šli proti čl. 6 GDPR. Naopak lze předpokládat, že zpracování

³⁶ Čl. 9 odst. 2 písm. g)

³⁷ ZAHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 978-80-7502-373-5. str.163-169

³⁸ Využívání zveřejněných osobních údajů | epravo.cz. (n.d.). EPRAVO.CZ. "Dostupné z: <https://www.epravo.cz/top/clanky/vyuzivani-zverejnenych-osobnich-udaju-109518.html>

³⁹ tamtéž

⁴⁰ tamtéž

zvláštních kategorií osobních údajů je i při splnění podmínek čl. 9 odst. 2 GDPR vždy třeba podřadit pod některý důvod zpracování dle čl. 6 odst. 1 GDPR, přestože v čl. 9 odst. 2 najdeme i výjimky, které nejsou explicitně uvedeny ve výčtu obecných důvodů a nemusí být tedy zřejmě, pod jaký důvod je můžeme podřadit.⁴¹

1.5. Správce a zpracovatel

Definice správce, je další definicí, kterou najdeme v čl. 4 bod) 7 GDPR. „*Správce, může být jak fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.*“⁴²

Hlavním role správce nastává při stanovení účelů a prostředků zpracování. Správce určuje účel, pro který budou osobní údaje zpracovávány a určuje také způsob, jakým se tak stane. Laicky řečeno, určí kdy, jak a proč se budou údaje zpracovávat, což z něj činí osobu, která je účastna u každého zpracování. V mnoha případech mu povinnost zpracování vyplývá ze zákona, jako například vedení povinné evidence pracovních úrazů a nemocí.⁴³ Účel a prostředky tedy stanovuje zákonodárce, subjekt v podobě správce se od nich nesmí odchýlit a musí dodržovat veškerá práva a povinnosti uvedená v GDPR anebo vnitrostátní legislativě. V postavení správce bývá nejčastěji zaměstnavatel, ale může to být i osoba, kterou za správce určí zákon. V případě zaměstnavatele, může být správcem buď celek v případě právnické firmy anebo fyzická osoba v případě živnostenské činnosti.⁴⁴

Zpracovatel je osoba, kterou může správce určit pro zpracování osobních údajů a ten následně jedná na základě pokynů správce a zpracovává údaje jeho jménem s tím, že provádí konkrétní operace zpracování údajů.⁴⁵ Zatímco správce má celkovou kontrolu nad zpracováním osobních údajů a je odpovědný za dodržování příslušných zákonů a předpisů o ochraně údajů, zpracovatel jedná na základě pokynů správce a musí dodržovat smluvní dohody a směrnice správce týkající se zpracování údajů. Povinnosti zpracovatele musí být konkretizovány ve

⁴¹ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer, 2019., s. 131, Právní monografie (Wolters Kluwer ČR). ISBN 978- 80-7598-587-3.

⁴² Čl. 4 odst. 7 GDPR a §5 zákona ZZOU

⁴³ FIALA, O. Kapitola I. Obecný úvod do GDPR. In: FIALA, GREPL, LICHNOVSKÝ 2019 op. cit., str. 17-20

⁴⁴ NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 90-92

⁴⁵ Čl. 4 odst. 8 GDPR

smlouvě nebo jiném právním aktu, a to jak při počátku zpracování údajů – jejich shromážděním a ukládáním, tak v případě jejich likvidace.⁴⁶

Správce údajů může být zároveň zpracovatelem, ale často to bývají i třetí osoby nezávislé na správci, jako např. v případě uzavření smluv mezi zaměstnavatelem a společností, která se zaměřuje na mzdové účetnictví. Zaměstnavatel v tomto případě v postavení správce poskytne mzdové firmě údaje, jaké mzdy a komu by měla vyplácet a mzdová firma poskytuje IT systém a ukládá osobní údaje zaměstnanců za účelem dalšího mzdového zpracování.⁴⁷

⁴⁶ Kdo je to správce údajů nebo zpracovatel údajů? (n.d.). Evropská komise. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_cs

⁴⁷ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Právo (ANAG). Olomouc: ANAG, [2017]. ISBN 978-80-7554-097-3.

2. Prameny práva

Jak již bylo napsáno výše, právo na ochranu osobních údajů bylo dlouhou dobu považováno za součást práva na soukromí. Jako samostatné právo se vyčlenilo až později v polovině 20. století, a to zejména jako reakce na vývoj moderních technologií a na rizika, která s sebou přinesla. V rámci této kapitoly, bych chtěla krátce nastínit historický vývoj práva na ochranu osobních údajů v návaznosti na klíčové mezinárodní dokumenty, které stanovily standardy pro toto právní odvětví. V druhé části této kapitoly bych se chtěla věnovat současným platným pramenům a jednotlivým zásadám dle GDPR.

2.1. Vývoj ochrany osobních údajů

Z hlediska vývoje ochrany osobních údajů je nutné zmínit dva nejvýznamnější mezinárodní dokumenty 20. století, a to Všeobecnou deklaraci lidských práv OSN z roku 1948 a Evropskou úmluvu o ochraně lidských práv a svobod vydanou Radou Evropy v roce 1950. Oba tyto dokumenty vznikaly po druhé světové válce a v podstatě reagovaly na její hrůzy. Zaměřovaly se tak na ochranu soukromí zejména proti zásahu veřejné moci a právo na ochranu osobních údajů chápaly, jako podmnožinu práva na soukromí.

Jako samostatné právo na ochranu osobních údajů se vyčlenilo až později, většinou se jeho vznik, jako samostatného právního odvětví datuje do 70 let 20. století od doby přijetí Úmluvy č. 108, která bude podrobněji rozebrána níže. V současné době je právo na ochranu osobních údajů jedním ze základních práv garantovaných na nejvyšších úrovních v předpisech s největší právní silou, stejně jako samotné právo na soukromí.

2.1.1. Všeobecná deklarace lidských práv

Všeobecná deklarace lidských práv je nezávazný dokument, který však stanovil základní rámec pro většinu mezinárodních lidskoprávních úmluv a dodnes je zřejmě nejznámějším katalogem lidských práv. Přestože deklarace inspirovala legislativní systémy ve všech částech světa, hodnoty v ní obsažené jsou hodnotami západních civilizací a již během procesu přijímání se stala terčem kritiky, zejména ze strany tehdejšího Sovětského svazu a jeho satelitů.⁴⁸

⁴⁸ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer, 2019., s.41-43, Právní monografie (Wolters Kluwer ČR). ISBN 978- 80-7598-587-3.

Tyto státy se ohrazovaly vůči individualistickému pojetí lidských práv, pravým důvodem, ale byla obava z využívání lidských práv západem jako diplomatického nástroje proti komunistickým zemím (deklarace vznikala v období stupňujícího se napětí během studené války).⁴⁹ I přes výhrady si však žádný stát nedovolil být přímo proti deklaraci, vzhledem k tomu, že reagovala na hrůzy a následky druhé světové, a tak se „pouze“ zdržely hlasování. Stejný postoj zaujalo i Československo, které vlivem politických změn po únoru 1948 nehlasovalo a obdobně se zachovala i Jihoafrická republika (pro neslučitelnost apartheidu s lidskými právy) nebo Saudská Arábie (kvůli výhradám ke svobodě vyznání).⁵⁰ Důvod, proč byla deklarace jen doporučujícího charakteru můžeme také hledat v nastupující studené válce. Komise OSN měla obavy, že by tehdejších čtyřicet osm členů nepodpořilo právně závazný dokument, což se nemýlila, a tak význam deklarace spočívá především v interpretaci, aplikaci a položení mezinárodních základů ochrany lidských práv.⁵¹

Deklarace byla prvním celosvětově významným dokumentem, který deklaroval právo na soukromí a z hlediska ochrany osobnosti má význam především čl. 12, který stanovuje že: „*Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům*“⁵² a čl. 23 stanovující právo na svobodu zaměstnání, ochranu proti nezaměstnanosti a uspokojivé pracovní podmínky.⁵³ Samozřejmě, pro její nezávazný charakter není možné se ochrany v deklaraci dovolávat.

2.1.2. Evropská úmluva o ochraně lidských práv a svobod

Jako reakce na Všeobecnou deklaraci lidských práv, byla v roce 1950 přijata Evropská úmluva o ochraně lidských práv a svobod, která již závazná byla a jejím zřejmě nejpodstatnějším ustanovením je čl. 19, kterým se zřizuje Evropský soud pro lidská práva se sídlem ve Štrasburku. Existence tohoto soudu má značné dopady na faktické využívání EÚLP ze strany jednotlivců. Stížnost k němu může podat

⁴⁹ tamtéž

⁵⁰ PRECLÍK, P. Šedesáté výročí Všeobecné deklarace lidských práv. em.muni.cz. (1. 2. 2009) Dostupné z: <https://www.em.muni.cz/udalosti/1325-sedesate-vyroci-vseobecne-deklarace-lidskych-prav> [cit. 18. března 2024]

⁵¹ *Vše o OSN: historie, struktura, financování*. V Praze: Informační centrum OSN, c2014. ISBN 978-80-86348-18-6.

⁵² Čl. 12 Všeobecné deklarace lidských práv.

⁵³ Čl. 23 Mezinárodního paktu o občanských a politických právech.

každý, kdo cítí, že jeho práva, včetně práva na soukromí byla porušena ze strany smluvního státu.

Pro ochranu soukromí je podstatný čl. 8 EÚLP, který zaručuje právo každého na respektování svého soukromého a rodinného života, obydlí a korespondence. Oba dokumenty upravují právo na soukromí obecně, jelikož právo na ochranu osobních údajů se v době vzniku dokumentů považovalo za jeho součást. V obdobném smyslu se vyjadřuje i rozsáhlá judikatura ESLP, která, jak bylo vyjádřeno výše, odmítla definovat pojem soukromí pro jeho složitost, a přestože nezakotvila právo na ochranu osobních údajů, z judikatury zřetelně vyplývá, že ho vnímala jako nedílnou součást práva na soukromí.⁵⁴

EÚLP reagovala na změny související s nárůstem nových technologií lépe než Všeobecná deklarace lidských práv, o jejíž modernizaci se spíše diskutovalo, než, aby se činily konkrétní kroky. EÚLP rozhodně pomohla výkladová praxe ESLP, prostřednictvím kterého se mohla rozvíjet.

2.1.3. Mezinárodní pakty

Všeobecná deklarace byla postavena na tzv. soft law a trvalo téměř 20 let, než se podařilo Valnému shromáždění OSN přenést její hodnoty do právně závazných dokumentů, které se staly součástí vnitřních právních řádů členských států. Byly to mezinárodní pakty o občanských a politických právech a Mezinárodní pakt o hospodářských, sociálních a kulturních právech, oba předložené k podpisu v roce 1966. Československá socialistická republika oba pakty podepsala 7. 10. 1968, ale souhlas s nimi vyslovilo až Federální shromáždění Československé socialistické republiky. K ratifikaci obou paktů, tak došlo až v roce 1976 a v platnost vstoupily ve formě vyhlášky ministra zahraničních věcí č. 120/1976 Sb.⁵⁵

Mezinárodní pakt o občanských a politických právech upravuje v několika ustanoveních právo na důstojné zacházení, svobodu, život a osobní bezpečnost. Z hlediska ochrany soukromí je nejpodstatnější čl. 17, kdy první odstavec vychází přímo z Deklarace a stanoví zákaz zasahování do soukromí jedince. Ve druhém odstavci uvedeného článku Paktu je stanoveno, že „každý má právo na zákonnou

⁵⁴ ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Právo (ANAG). Olomouc: ANAG, 2018. ISBN 978-80-7554-152-9. str. 13-15

⁵⁵ Mezinárodní pakt o občanských a politických právech a Mezinárodní pakt o hospodářských, sociálních a kulturních právech | Vláda ČR. Dostupné z: <https://vlada.gov.cz/cz/pracovni-a-poradni-organy-vlady/rfp/dokumenty/mezinarodni-pakt-o-obcanskych-a-politickych-pravech-a-mezinarodni-pakt-o-hospodarskych--socialnich-a-kulturnich-pravech-19852/>

ochranu proti (...) zásahům nebo útokům“⁵⁶ do soukromí. Z Paktu tak, na rozdíl od Deklarace, vyplývá pozitivní závazek smluvních států chránit soukromí prostřednictvím zákonů a jiných právních předpisů.⁵⁷

Mezinárodní pakt o hospodářských, sociálních a kulturních právech převzal úpravu sociálních práv z deklarace a má významný vliv na formování pracovního prostředí a pracovněprávní úpravy v členských státech. Vzhledem k tomu, že v době jeho ustanovení ještě stále neexistovala oddělená úprava ochrana osobních údajů, nezabývá se toliko ochranou soukromí na pracovišti a nedotýká se ani monitoringu, nicméně jeho podstatný vliv spočívá zejména ve stanovení základních principů fungování pracovního trhu.⁵⁸

2.1.4. Směrnice Rady OECD

OECD je Organizace pro hospodářskou spolupráci a rozvoj, která v současné době sdružuje třicet osm členských zemí a zaměřuje se na podporu hospodářského rozvoje a spolupráce mezi členskými státy. Založena byla sedmnácti státy v roce 1961 a Česká republika se stala členem v roce 1995. Organizace sehrála podstatnou roli v rozvoji mezinárodních standardů pro ochranu osobních údajů.

V roce 1980 vydala OECD historicky významnou Směrnicí Rady OECD o ochraně osobních údajů, která se stala prvním mezinárodním dokumentem, který stanovil základní principy ochrany osobních údajů, a to jak ve veřejném, tak soukromém sektoru. Kromě definic základních pojmů, bylo jejím největším přínosem stanovení základních zásad při nakládání s osobními údaji, a to i při neautomatizovaném nakládání, což níže uvedená Úmluva 108 učinila až v roce 2018. Tyto zásady a definice lze povětšinou považovat za platné i dnes, neboť byly dále přejímány pozdějšími právními dokumenty. Například pojem osobní údaj směrnice OECD definovala jako „*jakoukoliv informaci vztahující se k identifikované nebo identifikovatelné fyzické osobě*.“ Tuto definici následně přejala jak směrnice 95/46/ES (v čl. 2 písm. a) tak GDPR (v čl. 4 odst. 1). Rozdílně vnímala Směrnice OECD pojem subjekt údajů, který definovala, jako předmět údajů.

⁵⁶ Čl. 17 Mezinárodního paktu o občanských a politických právech.

⁵⁷ Pakt byl ratifikován Československou socialistickou republikou a vstoupil v platnost v roce 1976 ve formě vyhlášky ministra zahraničních věcí č. 120/1976 Sb.

⁵⁸ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Právní monografie (Wolters Kluwer ČR). Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. str. 47-49

Vzhledem k tomu, že se jednalo o osoby, není označení předmět úplně vhodné a je dobře, že byla definice následně změněna.⁵⁹

Směrnice měla za cíl poskytnout rámec pro ochranu soukromí a osobních údajů, který by mohl být použit v různých jurisdikcích po celém světě a od svého vzniku neprošla významnými aktualizacemi. Byla spíše považována za výchozí bod pro tvorbu národních zákonů a politik v členských státech OECD. Prvním právně závazným dokumentem většího významu v této oblasti se tak stala až Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (známá též jako Úmluva č. 108).

Úmluva č. 108 byla schválena Radou Evropy v roce 1981. Jedná se o historicky první dokument, který zohlednil význam ochrany osobních údajů v evropském rozměru. Úmluva se tak stala evropským právním nástrojem, na jehož základě začal celý následný proces mezinárodní kodifikace ochrany osobních údajů a soukromí jednotlivce. Tato úmluva však nebyla omezena jen na členské evropské státy, neboť jí podepsaly i zahraniční státy, jako je Mexiko, Senegal nebo Maroko. Vzhledem k tomu, že jde o úmluvu bez přímých právních následků, parlament České republiky jí ratifikoval a následně vyhlásil ve sbírce mezinárodních smluv v roce 2001.⁶⁰

Úmluva obsahuje definice základních pojmů, přičemž pojmy jako osobní údaj, správce nebo zpracování nikterak nezměnila a jejich význam zůstal zachován. Pojem zpracovatele původně Úmluva neobsahovala. Vzhledem k jejímu vzniku v průběhu 70. let musela být postupně modernizována a postupně se do ní doplňovaly definice, jako právě pojem zpracovatele anebo příjemce osobních údajů. Stejně tak zásada transparentnosti, nebo odpovědnosti nebyla původně obsažena a byla doplněna až s postupem času.⁶¹

Úmluva se nedá vymáhat před soudem ESLP, nicméně právě ESLP ve svých rozhodnutích označil ochranu osobních údajů jako nedílnou součást práva na

⁵⁹ Směrnice OECD o ochraně soukromí a přeshraničních tocích osobních údajů. [online]. 23. 9. 1980 [cit. 2024-03-18]. Dostupné z: <https://docplayer.cz/2620056-Prehled-smernice-oecd-o-ochrane-soukromi-a-preshranicnich-tocich-osobnich-udaju.html>

⁶⁰ ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Právo (ANAG). Olomouc: ANAG, 2018. ISBN 978-80-7554-152-9. str. 14-15

⁶¹ tamtéž

soukromí ve smyslu čl. 8 EÚLP a dovedil, že nesplnění pravidel podle Úmluvy může být porušením práva na soukromí ve smyslu zmiňovaného článku.⁶²

2.2. Unijní právní úprava

Obdobně jako mezinárodní právo, i unijní právo šlo postupnou cestou, kdy se primární právo EU nejprve věnovalo úpravě ochrany soukromí a postupně zvyšovalo míru ochrany v oblasti ochrany osobních údajů. V rámci primárního práva je stěžejním ustanovením čl. 16 Smlouvy o fungování Evropské unie, který nejenom zaručuje jednotlivcům právo na ochranu osobních údajů, ale taktéž v druhém odstavci zmocňuje evropský parlament a radu Evropy k přijímání pravidel o ochraně osob při zpracování osobních údajů. Toto zmocnění dalo vzniknout řadě právních norem sekundárního práva EU, které se ochraně osobních údajů věnují.

2.2.1. Směrnice 95/46/ES

Předchůdcem obecného nařízení známého také, jako GDPR byla směrnice 95/46/ES ze dne 24. 10. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Ta vznikla jako reakce na globalizaci společnosti, kdy začalo docházet k většímu předávání osobních údajů, jak mezi evropskými státy, tak do států třetích zemí. Jejím cílem mělo být sjednocení pravidel pro zacházení s osobními údaji a zajistit volný pohyb osobních údajů mezi státy. Směrnice nastavila poměrně vysokou úroveň ochrany osobních údajů, a přestože v sobě promítala řadu ustanovení Úmluvy č. 108 s úpravou ochrany osobních údajů se vypořádala komplexněji. Směrnice se vztahovala na automatizované a nově i neautomatizované zpracování osobních údajů.⁶³

Protože se jednalo o směrnici, která nebyla přímo aplikovatelná, byl dán požadavek na členské státy, aby do 3 let transponovaly do svých právních řádů příslušná ustanovení. Do českého právního řádu byla Směrnice implementována prostřednictvím novelizace č. 439/2004 Sb. ZOOÚ.⁶⁴

⁶² NONNEMANN, F. Modernizace Úmluvy 108, základního nástroje Rady Evropy pro ochranu osobních údajů. In: Epravo.cz [online]. 20. července 2018. [cit. 13. března 2024]. Dostupné z: <https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html>

⁶³ ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 22-25

⁶⁴ Čl. 32 odst. 1 Směrnice 95/46/ES.

Čl. 28 Směrnice stanovil členským státům povinnost zřídit na svém území dozorový orgán, který bude vykonávat dohled nad dodržováním předpisů. Tímto orgánem se v ČR stal Úřad pro ochran osobních údajů (ÚOOÚ), který byl zřízen dle § 2 ZOOÚ.⁶⁵

Významnou roli v oblasti ochrany osobních údajů sehrála i stanoviska a doporučení orgánu EU, zejména stanoviska pracovní skupiny pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, která je známá pod zkratkou WP29. Zřízena byla čl. 29 Směrnicí a jedná se o nezávislý poradní orgán Evropské komise.⁶⁶

Podstatná role Směrnice spočívala v sjednocení alespoň základního rámce úpravy ochrany osobních údajů, nicméně nebyla schopná dlouhodobě reagovat na čím dál tím rychlejší vývoj technologií a modernizaci prostředků ke zpracování osobních údajů. Vzhledem k tomu, že Směrnice přestala vyhovovat a jednotlivé úpravy členských států se v některých otázkách od sebe začaly lišit, byla nucena EU podniknout další kroky k cílenému sjednocování úprav. Tímto krokem bylo přijetí Obecného nařízení, které na rozdíl od Směrnice, svou formou přímo a bezprostředně zavazuje členské státy.⁶⁷

2.2.2. Obecné nařízení o ochraně osobních údajů

Nejpodstatnějším sekundárním pramenem EU je v současné době bezesporu nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. 4. 2016 obecně známé, jako GDPR. Jeho hlavním cílem bylo přizpůsobení právního rámce ochrany osobních údajů dnešní době a dosažení větší jednoty právního rámce ve všech zemích na které dopadá.⁶⁸

GDPR bylo pokračovatelem Směrnice a v recitálu č. 9 zmiňuje, že jsou v úpravě převzaty cíle a zásady ze Směrnice. I proto se obsahově GDPR od Směrnice příliš neliší. Základní struktura zůstává zachována a dosavadní instituty a ustanovení GDPR spíše zpřesňuje nebo lehce pozměňuje. V čl. 68 GDPR dochází k nahrazení pracovní skupiny WP29 nově zřízeným Evropským sborem pro

⁶⁵ Čl. 28 odst. 1 Směrnice 95/46/ES.

⁶⁶ ŽŮREK, Jiří. Praktický průvodce GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN: 978-80-7554-152-9, s. 15-17

⁶⁷ tamtéž

⁶⁸ Základní příručka k ochraně osobních údajů: Obecné nařízení [cit. 12. 3. 2024] Dostupné z: <https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju>

ochranu osobních údajů, který oproti předchozí skupině má rozšířené pravomoci, zejména v případě sporů, kdy může rozhodovat spory mezi dozorovými úřady.

Obecné nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na manuální zpracování osobních údajů v případě, že jsou tyto údaje obsaženy v evidenci nebo do ní mají být zařazeny.⁶⁹ Nevztahuje se poté na oblasti, které jsou dány do kompetencí jednotlivých států, jako je např. zajišťování národní bezpečnosti a činnosti, které spadají pod zahraniční politiku anebo zpracování údajů, které provádějí příslušné orgány za účelem vyšetřování, odhalování anebo stíhání trestných činů.⁷⁰

2.3. Vnitrostátní právní úprava

Právo na soukromí je jedním ze základních práv, která jsou chráněna na nejvyšší úrovni, a to Listinou základních práv a svobod, která byla vyhlášena jako nedílná součást ústavního pořádku usnesením předsednictva České národní rady. Listina nezmiňuje přímo ochranu osobních údajů, ale zaměřuje se na ochranu soukromí, které je základním právem. Nicméně, protože je ochrana osobních údajů spjata a je prakticky součástí práva na ochranu soukromí, je potřebné na začátku této kapitoly zmínit čl. 7 odst. 1, čl. 10⁷¹ a čl. 13 LZPS.⁷² Tyto články garantují nedotknutelnost osoby a jejího soukromí a také právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a jména. Tato ustanovení, respektive práva se mohou dostat do střetu s právem na informace zaručeném v čl. 17 odst. 1 LZPS. V případě střetu základních práv je vždy nutné provést test proporcionality, jak uvádí i GDPR, právo na ochranu osobních údajů musí být vždy posuzováno v souvislosti s okolnostmi a musí být v rovnováze s dalšími základními právy⁷³

Základním právním předpisem, který upravuje pracovněprávní vztahy je zákoník práce. Přestože se jedná o stěžejní pracovněprávní předpis a v podstatě

⁶⁹ Čl. 2 odst. 1 a 2 GDPR

⁷⁰ Základní příručka k ochraně osobních údajů: Obecné nařízení [cit. 12. 3. 2024] Dostupné z: <https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju>

⁷¹ 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.“

⁷² 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.“

⁷³ Desatero omylů. [cit. 14. 3. 2024] Dostupné z: <https://uoou.gov.cz/verejnost/qa-otazky-a-odpovedi/desatero-omylu>

komplexně upravuje vztahy mezi zaměstnancem a zaměstnavatelem, otázkám ochrany soukromí se věnuje jen v pár vybraných ustanoveních. Podstatným je §316, který se mimo jiné týká kontroly a sledování zaměstnanců. Další paragrafy zákoníku práce budou postupně rozebrány v rámci této práce, zejména v kapitole, která se týká ochrany osobních údajů v jednotlivých fázích pracovního poměru, pro počáteční fázi výběrového řízení je to např. § 30 odst. 2, který stanovuje, jaké informace může zaměstnavatel požadovat. Úzké propojení tohoto ustanovení můžeme najít v § 12 zákona o zaměstnanosti, který upravuje, že zaměstnavatel sice má nárok na informace, ale rovnou obsahuje výčet těch, které jsou zakázané.

V § 4 zákoníku práce je zmíněn vztah mezi zákoníkem práce a občanského zákoníku, který zmiňuje ochranu osobnosti hned v úvodních ustanoveních. Blíže se pak ochraně osobnosti věnuje OZ v ustanovení § 81, který upravuje vybrané aspekty osobnosti člověka, ať už se jedná o jeho podobu anebo soukromí, o právo na duševní a tělesnou integritu či ochranu lidského těla. Přestože výčet v občanském zákoníku není taxativní, je pojat velmi detailně a jen těžko bychom hledali další práva, která by v těchto ustanoveních nebyla zmíněna.⁷⁴ 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.⁷⁵

Vzhledem k tomu, že zákoník práce i zákon o zaměstnanosti dává zaměstnavateli právo na osobní údaje svých zaměstnanců, je další podstatnou úpravou zákon o zpracování osobních údajů, který nahradil zákon o ochraně osobních údajů č. 101/2000 Sb. který byl výchozí normou pro zpracování osobních údajů. ZZOU se zabývá spíše specifickými situacemi a upravuje ty otázky, u kterých GDPR předpokládá, že se jimi budou členské státy samy prostřednictvím vnitrostátních právních předpisů zabývat. Jedná se tak o situace, které mají předcházet a vyvarovat se trestné činnosti při zpracování osobních orgánů anebo určení věkové hranice pro děti při udělení souhlasu.⁷⁶

⁷⁴ ZAHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 978-80-7502-373-5.

⁷⁵ 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

⁷⁶ ŽŮREK, Jirí. *GDPR v personalistice. Práce, mzdy, pojištění*. Olomouc: ANAG, [2019]. ISBN 978-80-7554-210-6. str. 12-14

Zákoník práce, zákon o zaměstnanosti a zákon o zpracování osobních údajů jsou zcela zásadní zákony vzhledem k tématu práce, ale je zde mnoho dalších právních předpisů, jak stejné anebo nižší právní síly. Za zmínku stojí např. zákon o rovném zacházení a o právních prostředcích ochrany před diskriminací (antidiskriminační zákon), zákon o inspekci práce, zákon o přestupcích a dále zákony, které vymezují předpoklady pro výkon určitých povolání, kde přímo či nepřímo určují rozsah osobních údajů, které je zaměstnavatel oprávněn vyžadovat. Jedná se například o zákon o státní službě, který v řadě ustanovení upravuje kontrolu státních zaměstnanců a neobsahuje ustanovení, které by bylo možné považovat za obdobu § 316 zákoníku práce. Vzhledem k tomu, že vztah zákona o státní službě a zákoníku práce je založen na vztahu delegace, ustanovení § 316 zákoníku práce by bylo na služební poměr aplikovatelné pouze za předpokladu, že by na něj zákon o státní službě přímo odkazoval. Otázkou tedy zůstává, zda je zaměstnavatel oprávněn zaměstnance podrobit kontrole, která by odpovídala kontrole dle předmětného ustanovení zákoníku práce a pokud ano, podle jakých právních předpisů bude povinen postupovat.⁷⁷

2.4. Zásady zpracování osobních údajů

Právní zásady můžeme obecně popsat jako určitá východiska, vůdčí ideje anebo obecná pravidla, která se promítají do celé úpravy konkrétních právních oblastí a pomáhají s pochopením jejich podstaty. Právní zásady slouží k mnoha účelům, jedním z nich je pomocná role, při výkladu a interpretaci jednotlivých článků GDPR. Kromě toho se jedná také o přímo vynutitelná pravidla, za jejichž porušení může být udělena sankce na základě čl. 83 odst. 1 a čl. 83 odst. 5 písm. a) GDPR. Vzhledem k tomu, že se jedná o základní principy, jejich význam je podstatný také v rámci legislativních procesů členských států, a to nejenom v rámci adaptačních zákonů, ale také v dalších příslušných předpisech. Zásady v tomto ohledu mají svou podstatnou roli, neboť již v roce 2011 se Soudní dvůr Evropské unie zakázal členským státům přidávat nové zásady anebo ukládat další povinnosti nad rámec zásad, jež by měly za následek změnu jejich působnosti.⁷⁸

⁷⁷ ZÁHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 19-21

⁷⁸ MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer, 2019., s. 155, Právní monografie (Wolters Kluwer ČR). ISBN 978- 80-7598-587-3

Zásady pro zpracování osobních údajů jsou fakticky stanovené povinnosti pro správce a zpracovatele, jejichž ustanovení můžeme nalézt v čl. 5 GDPR. Vzhledem k vyjádření SDEU se jedná o taxativní seznam a jednotlivé zásady jsou v čl. 5 detailně rozepsány. Jedná se o poměrně ojedinělý krok zákonodárce, neboť nebývá zvykem, aby byly zásady takto přesně a detailně vymezeny, v případě GDPR se však jedná o relativně logický krok, vzhledem k historické genezi. Jedná se totiž o dlouhodobou praxi explicitního popisování zásad v podstatných dokumentech zaměřujících se na ochranu osobních údajů. Hlavní zásady byly totiž vtěleny už do Úmluvy č. 108 a odtud následně převzány i do znění čl. 6 směrnice 95/46/ES, která byla přímým předchůdcem GDPR.⁷⁹

Další neobvyklým krokem v této úpravě, je přímo upravena povinnost správce osobních údajů se jimi řídit. Podle čl. 5 odst. 2 GDPR je stanovena výslovná odpovědnost správců za dodržování zásad, a to včetně schopnosti prokázat, že k jejich dodržování dochází. Vzhledem k tomu, že se jedná o povinnost správců dodržovat zásady, jako celek, jedná se o komplexní systém, kdy musí kromě jiného zajistit bezpečnost údajů, informovat subjekty o účelu poskytování údajů, dbát na jejich aktuálnost a spolupracovat s dozorovými úřady, pokud dojde k incidentu, který by mohl bezpečnost a zpracování osobních údajů narušit.

2.4.1. Zásada zákonnosti

Zásada zákonnosti je uváděna společně se zásadou korektnosti a transparentnosti v čl. 5 odst. 1 písm. a), který udává povinnost správci, aby byly údaje zpracovávány vždy korektně, zákonně a transparentním způsobem. Vzhledem k tomu, že se jedná o první zásady, je zde patrný úmysl zákonodárce klást na ně největší důraz.

Autorka se rozhodla tuto zásadu vymezit jako první v rámci samostatné podkapitoly, čistě kvůli větší přehlednosti a také proto, že se přeci jen domnívá, že svým významem je od zbylých dvou lehce odlišná. V širším slova smyslu vyjadřuje povinnost správce dodržovat právní předpisy, což znamená zejména pravidla uvedená v GDPR, ale také vnitrostátní doprovodnou legislativu. V užším slova smyslu zásada znamená, že zpracování osobních údajů je zákonné pouze tehdy, pokud existuje alespoň jeden z taxativně stanovených právních titulů pro

⁷⁹ JANEČKOVÁ, Eva. GDPR: praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. str. 3-9

zpracování osobních údajů. Ty najdeme upraveny v čl. 6 odst. 1 písm. a) až f) GDPR anebo pro zvláštní kategorii osobních údajů v čl. 9 odst. 2 GDPR.⁸⁰

Pokud správce zjistí, že mu pro zpracování údajů nestačí žádný z uvedených prvních důvodů je povinen okamžitě přestat osobní údaje zpracovávat. Pokud tedy již v prvním kroku, dojdeme k tomu, že pro zpracování údajů nemáme žádný právní důvod, k ostatním zásadám se ani nedostaneme, a to staví zákonnost na pomyslný piedestal. Absence právního titulu má za následek porušení zásady legality a pro nezákonnost má být celý proces zpracování ukončen a osobní údaje zlikvidovány anebo anonymizovány.⁸¹

2.4.2. Zásada korektnosti a transparentnosti

Jak již bylo řečeno, všechna zpracování osobních údajů je možné realizovat pouze na základě zákonných titulů, které musí být dostatečně specifické, korektní a transparentní. Zásada transparentnosti se skládá z několika prvků, které mají společně napomoci vytvořit důvěru mezi správcem a subjekty. Aby tato důvěra fungovala, je potřeba, aby správce dodržoval určité postupy, které budou dostatečně otevřené ve smyslu informativnosti, aby subjekty mohly tyto postupy kontrolovat a v případě potřeby se bránit proti nezákonnému nakládání s údaji. Transparentnost tedy především vyžaduje, aby správce údajů veškerá sdělení a informace vůči subjektům činil stručně a srozumitelně, ve snadno přístupné podobě a za použití jednoduchých jazykových prostředků. Vzhledem k tomu, že jde o získání důvěry, je zcela logické, že poskytnuté informace musí být pravdivé, přestože toto explicitně GDPR neuvádí.⁸²

Správce údajů by se také měl vyhnout přehlčení subjektů informacemi. Požadavek srozumitelnosti může být někdy chápán docela obtížně, nicméně by se mělo jednat o takové výrazové prostředky, kterým porozumí průměrná osoba. Platí zde právní domněnka, že takovou osobou je každý, kdo je svéprávný, má rozum průměrného člověka a z jeho chování vyplývá, že je schopen ho používat. Pokud není možné dané informace sdělit subjektům stručně, volí se tkz. vícevrstvý přístup, kdy jsou subjektům příslušné dokumenty a informace podávány po dávkách, aby

⁸⁰ Čl. 6 a čl. 9 GDPR

⁸¹ JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. str. 3-9

⁸² Pracovní skupina WP 29. Pokyny k transparentnosti podle nařízení 2016/679. (WP260) přijaté dne 29. listopadu 2017. [online]. [cit. 12. 3. 2024]. Dostupné z: <https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/k-transparentnosti.pdf>

měli čas je v klidu prostudovat a plně pochopit. V případě vícevrstvých dokumentů, by ten první měl obsahovat nejvíce stěžejní informace, kterými jsou zejména to, kdo je správcem, jaký je účel zpracování a jaké údaje budou zpracovány. Neméně podstatným sdělením jsou i případná rizika, které mohou se zpracováním nastat.⁸³

GDPR v čl. 88 odst. 2 uvádí transparentnost jako jeden z nejdůležitějších prvků zajišťujících ochranu lidské důstojnosti a základních práv zaměstnanců v souvislosti s výkonem zaměstnání. Splnění povinnosti shromažďovat osobní údaje pouze otevřeně, tedy nikoli pod záminkou jiného účelu, nebo jiné činnosti je podstatnou podmínkou efektivní ochrany osobních údajů zejména proto, že na základě uvedených informací se může subjekt aktivně podílet na ochraně svých údajů.⁸⁴

Další složkou transparentnosti je dostupnost informací. Ať už dochází k předávání základních informací o zpracování údajů v digitální nebo nedigitální podobě, vždy je podstatné pravidlo dostupnosti dodržovat. Nejedná se však jen o to, že by dokument měl být snadno přístupný a lehce dohledatelný, je zde také požadavek na to, aby subjekt věděl, jakým způsobem a kde základní informace získá.

Zásada korektnosti ukládá správcům povinnost zpracovávat údaje způsobem, který je běžný a očekávatelný. Jinými slovy by se tato zásada mohla nazvat zásadou adekvátnosti anebo spravedlnosti. Vzhledem k tomu, že ze strany správců nemá docházet k zastíracím jednáním, má se jednat o zpracování takovým způsobem, který se zakládá na pravdivých skutečnostech a nemá negativní dopady na dotčené subjekty. Správce by se měl držet stanoveného účelu, aby subjekt údajů nebyl zaskočen tím, jakým způsobem jsou jeho osobní údaje používány. Na rozdíl od transparentnosti, se GDPR touto zásadou téměř nezabývá, k jejímu porušení však nejčastěji dochází právě kvůli nedostatečné informovanosti.⁸⁵

⁸³ JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. str. 3-9

⁸⁴ Recitál č. 39 a č. 40 GDPR

⁸⁵ Pracovní skupina WP 29. Pokyny k transparentnosti podle nařízení 2016/679. (WP260) přijaté dne 29. listopadu 2017. [online]. [cit. 22. 3. 2024].

Dostupné z: <https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/k-transparentnosti.pdf>

2.4.3. Zásada integrity a důvěrnosti

Vymezení této zásady můžeme najít v čl. 32 GDPR, který klade povinnosti na správce a zpracovatele zajistit, aby osobní údaje byly chráněny před neoprávněným přístupem ze strany třetích osob. To zahrnuje implementaci bezpečnostních opatření, jako jsou například hesla, šifrování jednotlivých dat, odpovídající hardware a software, anebo přístupná IT podpora a omezený přístup k údajům pouze oprávněným osobám. Další praktické dopady této zásady můžeme najít v tom, že přístup k údajům je omezen na nezbytně nutnou dobu pro vykonání práce a premisa, že je vždy lepší přijmout přísnější bezpečnostní politiku než riskovat, že dojde k úniku anebo poškození údajů.⁸⁶

Nestačí však tato opatření pouze zavést, součástí této zásady je také požadavek na pravidelné testování a hodnocení účinnosti zavedených opatření. Správce a zpracovatel užití k ochraně údajů takové prostředky, které jsou dle nich dostatečné pro hrozící riziko, přičemž je vždy nutné vycházet z kategorie zpracovávaných údajů, anebo případného počtu dotčených subjektů údajů, kteří by mohly být po úniku dat ohroženy. U každého správce tak bude opatření odlišné, právě s ohledem na povahu, rozsah a účely daného zpracování, nehledě na to, že správce musí reflektovat stav techniky, což je značně dynamický pojem, který se nevztahuje, jen na samotnou techniku, ale i na organizační opatření.⁸⁷

2.4.4. Zásada přesnosti

Zásada přesnosti se netýká toliko vztahu a vybudování důvěry mezi správcem a subjektem, jako spíše samotných osobních údajů. Vyplývají z ní povinnosti pro správce zajistit přesnost a aktuálnost údajů, které zpracovávají a přijmout veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.⁸⁸

Pokud by byly údaje nepřesné nebo neúplné, mají jednotlivci právo požadovat jejich opravu. Toto právo opět vyplývá z požadavku na otevřenost a

⁸⁶ JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. str. 3-9

⁸⁷ EDPB. Pokyny 4/2019 k článku 25 Záměrná a standardní ochrana osobních údajů. Verze 2.0. ze dne 20. října 2020, [cit. 29. 3. 2024]. Dostupné z: <https://uouu.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-420-19-clanku-25-zamer-na-a-standardni-ochrana-osobnich-udaju.pdf>

⁸⁸ Čl. 5 odst. 1 písm. d) GDPR

snadný přístup k údajům, kdy subjekty mohou lehce ověřit, že jsou jejich údaje aktuální. Kromě požadavku na údaje, klade zásada další povinnosti na správce, kteří mají přijmout veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné vymazal, neboť platí premisa, že je lepší nemít žádný údaj než mít údaj chybný. Přestože jsou požadavky na přesnost docela přísné, jak při jejich shromažďování, tak v průběhu zpracování, nařízení ani současná úprava konkrétně nestanovuje, jakým způsobem má být tato povinnost zajišťována. Jako nesprávné údaje můžeme chápat nejenom údaje vyloženě chybné, ale i nepřesné nebo nekompletní. Míru přesnosti a požadavek aktualizace je třeba vždy vykládat vzhledem k účelu, pro který jsou osobní údaje zpracovávány.⁸⁹

Jedním z vhodným řešením může být doporučení zaměstnavatele směrem k zaměstnanců, aby nahlašovali změny osobních údajů (zejména těch, které jsou v čase proměnlivé, jako příjmení v souvislosti se sňatkem nebo naopak rozvodem, změny bydliště nebo kontaktních adres). Dalším způsobem jsou průběžné kontroly např. na základě notifikačních emailů, které nabádají subjekty, aby potvrdily, že jsou jejich údaje aktualizované.⁹⁰

2.4.5. Zásada minimalizace údajů

Tato zásada je úzce spjata s principem účelového omezení, která je formulována v čl. 5 odst. 1 písm. f) a podle které musí být údaje „shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný“. Správce musí účel stanovit dostatečně konkrétně, a ne moc široce, aby nedošlo k jeho záměně s jiným účelem. Je nepřípustné, aby správce shromáždil údaje k určitému účelu a následně je zpracoval k jinému. Požadavek na legitimitu poté znamená soulad s právními normami. Tímto ustanovením se zamezuje libovůli správců a obcházení platné právní úpravy.⁹¹

Zásada minimalizace údajů poté vyžaduje, aby pro stanovený účel shromažďovali správci pouze ty osobní údaje, které jsou nezbytné. V čl. 5 odst. 1 písm. c). GDPR je zásada minimalizace popsána tak, že poskytnuté údaje mají být

⁸⁹ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s. 204

⁹⁰ ŽŮREK, J. GDPR v personalistice. Olomouc: ANAG, 2019. ISBN 978-80-7554-210-6 s. 47-48

⁹¹ JANEČKOVÁ, Eva. GDPR: praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. str. 3-9

„přiměřené, relevantní a omezené na nezbytný rozsah k účelu, pro který jsou zpracovávány“.⁹²

Pro splnění podmínky přiměřenosti potřebujeme přesné vymezení minimálního rozsahu konkrétních osobních údajů, které budou v daném případě potřeba k naplnění stanoveného účelu. Tato kontrola, zda je údaj potřebný nebo nikoliv, by měla probíhat ve vztahu ke každému z nich. Přiměřenost je důležitá pro minimalizaci rizika zneužití.

2.4.6. Zásada omezení uložení

Kvůli zachování bezpečnosti a zamezení případnému vzniku rizika, by zpracovatelé neměli uchovávat osobní údaje déle, než je nezbytně nutné. Společně s kontrolou aktuálnosti údajů je tak zapotřebí, aby docházelo i ke kontrolám, zda s plynutím času neztrácí údaje svůj smysl.

V této zásadě je vyjádřena přímá vazba účelu zpracování na dobu zpracování. Správce je povinen tuto dobu sám určit, a to přiměřeným způsobem. Za toto své rozhodnutí je následně odpovědný. Doba zpracování může být určena vymezeným časovým obdobím anebo na dobu trvání právního vztahu. Případně může být prodloužena o dobu nezbytnou k vypořádání vzájemných práv. Výjimkou je, pokud by byla doba uložení konkrétně omezena zvláštním zákonem.⁹³

Pokud chce správce zpracovávat údaje i po této době, musí se buď jednat o některou z výjimek uvedených v čl. 89 odst. 1, kdy je možné prodloužit dobu zpracování, pokud se jedná o účely archivace ve veřejném zájmu, pro účely historického nebo vědeckého výzkumu nebo pro statistické účely anebo musí v souladu s touto zásadou údaje anonymizovat, čímž v podstatě osobními údaji být přestanou.⁹⁴

⁹² FIALA, O. Kapitola I. Obecný úvod do GDPR. In: FIALA, GREPL, LICHNOVSKÝ 2019 op. cit., str. 5-15.

⁹³ tamtéž

⁹⁴ Čl. 89 odst. 1-4 GDPR

3. Práva a povinnosti

Rozdělení rolí v pracovněprávních vztazích je poměrně jednoznačné. Na jedné straně máme zaměstnavatele jako správce a na druhé zaměstnance jako subjekt údajů. Obě strany fungují za cílem ryze ekonomickým, a to je výkon závislé práce. Zaměstnanec, kterým může být pouze fyzická osoba vykonává pro zaměstnavatele práci, za kterou je odměněn. Z postavení obou stran vyplývají vzájemná práva a povinnosti. Cílem GDPR bylo mimo jiné nastolení důvěry, odstranění administrativní zátěže a důsledné zpracování osobních údajů a v souladu.⁹⁵

Ústřední základy důležité pro zákonné zpracování jsou obsaženy v základních zásadách, které byly uvedeny výše. Zásady plní funkci všudypřítomných pravidel, které prostupují všemi zpracovatelskými činnostmi. Bez znalosti zásad nemůže správce docílit toho, že jeho zpracování bude zákonné. V této kapitole bych na zásady chtěla navázat a věnovat se povinnostem a právům oběma stranám pracovního poměru.

3.1. Povinnosti zaměstnavatele

Hlavní a nejspíše i stěžejní povinností správce je stanovení právního titulu pro zpracování údajů, neboť zpracování je dovoleno pouze za podmínky, že správci pro danou zpracovatelskou činnost svědčí alespoň jeden z právních titulů. Existence řádného právního titulu je základem jakéhokoliv zpracování osobních údajů a správce musí být vždy schopen jej doložit, neboť v případě sporu je důkazní břemeno na jeho straně.

Otázka, na základě jakého titulu budou dané osobní údaje zpracovávány může být často sporná, nicméně její zodpovězení je z hlediska povinnosti správce i práv subjektů nezbytné. Každý správce by měl mít ještě před samotným začátkem zpracování dostatečný přehled o tom, který právní titul bude základem činnosti s údaji. Se stanovením účelu souvisí i stanovení prostředků a procesů zpracovávání osobních údajů, které musí být zvoleny tak, aby garantovaly dostatečné zabezpečení.⁹⁶

⁹⁵ BURIAN, David. RADICOVA, Zuzana. K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR). In: Právní prostor [online]. 25. 2. 2016 [cit. 20. 3. 2024].

⁹⁶ ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 163

Vzhledem k tomu, že pracovní vztahy jsou vztahy dobrovolné a založené na základě smlouvy, ať už pracovní anebo o konání dohod mimo pracovní poměr je nejčastějším právním titulem zejména zpracování, které je nezbytné pro splnění smlouvy dle čl. 6 odst. 1 písm. b).

Dalším podstatným důvodem je plnění povinností, která na zaměstnavatele v roli správce klade zákon. Pod tyto povinnosti lze podřadit vedení evidence odpracované doby, anebo plnění povinností vůči zdravotnímu nebo důchodovému pojištění.⁹⁷

Posledním důvodem pro zpracování pod písm. f) je zpracování osobních údajů z důvodu oprávněného zájmu ať už svého anebo třetí strany. Oprávněný zájem může zaměstnavatel využít pouze za předpokladu, že jeho zájem nepřeváží práva a zájmy subjektu údajů. Sám o sobě je oprávněný zájem neurčitý pojem, který musí zaměstnavatel blíže definovat ve vztahu ke konkrétní situaci. Jakmile je zájem definovaný, je nutné posoudit dle výše uvedeného, jeho podstatnost oproti zájmům subjektu. To provede zaměstnavatel tkz. balančním testem (test proporcionality), při kterém bude posouzena vhodnost a potřebnost zpracovávaných údajů, vzhledem k účelu, kterého má být dosaženo.⁹⁸

3.1.1. Zpracování na základě souhlasu

Pokud zpracování nelze podřadit pod právní důvody čl. 6 bod b) až f) GDPRP je možné zpracovávání údajů považovat za zákonné, bude-li podloženo souhlasem osoby, jejíž údaje se zpracovávají. Využití souhlasu, jako právního titulu je možné jen výjimečně a obnáší různá omezení.

Souhlas musí být svobodný, konkrétní, informovaný a jednoznačný, jak uvádí definice v čl. 4 bod. 11 GDPR. Zejména informovanost je podstatnou složkou souhlasu, neboť subjekt musí vědět komu, za jakým účelem a v jaké míře souhlas poskytuje. Získání souhlasu pak musí proběhnout v dobrovolném a svobodném projevu vůle, a to před zahájením zpracování osobních údajů. Dodatečný souhlas v žádném případě nezhojí předchozí nelegitimní chování zaměstnavatele.⁹⁹

⁹⁷ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, s. 195

⁹⁸ Recitál 47. GDPR

⁹⁹ Čl. 4 odst. 11 GDPR a recitál 32 GDPR

V čl. 4 se nedozvíme o formě, jakou má souhlas mít. V odůvodnění uvádí GDPR všechny možné formy, jak písemnou, elektronickou, tak ústní. Jediná forma, která není dostatečná je konkludentní. Souhlas vyjádřený mlčky nebo nečinností by neměl být brán v potaz, vzhledem k tomu, že má být konkrétní a dostatečně jednoznačný. Ústní forma souhlasu také není ideální, přestože jí GDPR připouští. Zaměstnavatel nese důkazní břemeno, musí prokázat, že mu byl souhlas udělen a v případě ústní formy je toto prokázání téměř nemožné. Proto se doporučuje zajištění souhlasu v písemné, případně elektronické podobě, kdy tento dokument bude od ostatních dostatečně odlišný.¹⁰⁰

Subjekt může svůj souhlas kdykoliv odvolat a toto odvolání musí proběhnout ve stejné formě anebo vyšší formě, než byl poskytnut souhlas. V případě písemného souhlasu musí být forma odvolání také písemná. Pokud by byl souhlas udělen slovně, je možné ho odvolat ústně i písemně.¹⁰¹

Problematika souhlasu spočívá v tom, že ho zaměstnavatelé často užívají nadbytečně a také je otázkou, nakolik je souhlas skutečně svobodný. Podle recitálu 42 GDPR nemůže být souhlas považován za svobodný, pokud nemá subjekt možnost odmítnout anebo ho odvolat, aniž by byl poškozen. Z nerovného postavení stran pracovněprávního vztahu zcela objektivně vyvstává možnost ať už otevřeného anebo skrytého nátlaku zaměstnavatele na stranu zaměstnance. Zaměstnanec může získat dojem, že pokud souhlas neposkytne bude tím ohrožen jeho kariérní růst nebo mzdové ohodnocení. Nadřízená pozice zaměstnavatele mu z pohledu zaměstnance dává dostatečný respekt, k tomu, aby se bál oponovat v případě, kdy souhlas udělit nechce. Stejně tak může zapůsobit pracovní prostředí okolo zaměstnance. Jen málo pravděpodobnou se mi jeví situace, kdy by zaměstnanec odmítnul využití své fotografie, zatímco všichni ostatní souhlasí a podpis před začátkem akce, z které mají být fotografie použity udělí v podstatě proti své vůli.¹⁰² Právě pro nerovné postavení stran by mělo být zpracování na základě souhlasu zastoupeno jen v omezené míře.

Z výše uvedeného vyplývá, že by se udělení souhlasu mělo vztahovat pouze na situace, které nemají velkou důležitost. V rámci běžného pracovněprávního

¹⁰⁰ Náležitost souhlasu se zpracováním osobních údajů. Úřad pro ochranu osobních údajů [online]. [cit. 2024-11-03]. Dostupné z: <https://uoou.gov.cz/verejnost/zakladni-priruccka-k-ochrane-udaju>

¹⁰¹ Čl. 7 odst. 1 a 2 GDPR

¹⁰² ŽŮREK, Jiří. GDPR v personalistice. Olomouc: ANAG, [2019]. Práce, mzdy, pojištění. ISBN 978-80-7554-210-6.

vztahu se může jednat např. o uveřejňování fotografií na webových stránkách zaměstnavatele. Pokud zaměstnanec odmítne, jen těžko by to mohlo mít dopad na výkon jeho práce anebo na povinnosti, které musí zaměstnavatel konat na základě pracovní smlouvy anebo ze zákona.

Před zahájením zpracování osobních údajů na základě souhlasu by prvotně měl správce posoudit, zda konkrétní záměr nelze podřadit pod některý z právních titulů podle čl. 6 písm. b) až f) GDPR, než přistoupí k použití souhlasu. Může se stát i situace, kdy správce dodatečně zjistí, že vyžadoval souhlas i tam, kde měl využít jiných právních titulů.¹⁰³ Logickým postupem by bylo odvolání souhlasu a využití správného právního titulu, ale za stanoviska a ÚOOÚ č. 3/2014 můžeme usuzovat, že by tento postup nebyl správný. Po odvolání souhlasu by obecně nemělo dojít ke změně právního titulu, protože základní princip možnosti odvolatelnosti souhlasu je zastavení zpracování, které je na něm založeno. Řešením situace by tak bylo dostatečné informování subjektu, o chybě zpracování, s tím že subjekt souhlas neodvolá, aby neměl za to, že s údaji nebude dále zacházeno a zaměstnavatel plynule přejde ze souhlasu na jiný právní titul.¹⁰⁴

V případě, kdy má správce správný právní titul pro zpracování a stejně požaduje souhlas se jedná o nadbytečnost, která je vnímána jako porušení povinnosti zaměstnavatele. Souhlas zaměstnance se zpracováním by neměl být pořizován, jako pojistka a pracovní smlouvy zaměstnavatelů by tak neměly obsahovat dokumenty označené jako generální souhlas ke zpracování údajů. Tento postup je špatný z mnoha důvodů, nejenom kvůli nadbytečnosti, ale také kvůli klamání subjektu, který může získat dojem, že ke zpracování dochází na základě jeho souhlasu, a ne kvůli pracovní smlouvě anebo plnění zákonných povinností.¹⁰⁵

3.1.2. Informační povinnost

Informační povinnost pro správce vychází ze zásady transparentnosti a vyžaduje, aby všechny informace a všechna sdělení týkající se zpracování osobních

¹⁰³ Šilhánková, I., & Hanák, J. (2021, únor 10). Nadbytečný souhlas se zpracováním osobních údajů | epravo.cz. EPRAVO.CZ. [cit. 11. 3. 2024] Dostupné z: <https://www.epravo.cz/top/clanky/nadbytecny-souhlas-se-zpracovanim-osobnich-udaju-v-pracovnepravnich-vztazich-jak-situaci-vyresit-112582.html>

¹⁰⁴ Stanovisko č. 3/2014. K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informačních povinností. Úřad pro ochranu osobních údajů [online]. Úřad pro ochranu osobních údajů, © 2014,, s. 3 [cit. 11. 3. 2024]

¹⁰⁵ ZHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 139

údajů byly snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků. Zaměstnavatel by tak měl volit vhodné jazykové a informační prostředky k tomu, aby subjekt, kterým může být, jak uchazeč, tak zaměstnanec, informoval o tom, za jakým účelem, jakým způsobem a v jakém rozsahu, kým a jaké údaje budou zpracovávány.¹⁰⁶ V GDPR je informační povinnost upravena v čl. 12 až 14, kdy dává zaměstnavateli povinnost přijmout taková opatření, aby poskytl subjektu údajů stručným, transparentním a snadno přístupným způsobem veškeré informace. V případě aktualizace údajů anebo dokumentu musí tuto skutečnost zaměstnavatel dát taktéž zaměstnancům na vědomí.

Informační povinnost najdeme i v § 8 ZZOÚ, kdy pokud dochází ke zpracování údajů na základě § 5 ZZOÚ, tedy kvůli plnění povinnosti uložené zákonem, anebo ve veřejném zájmu, je toto odůvodnění samo o sobě dostatečně srozumitelné.¹⁰⁷

3.1.3. Povinnost zabezpečit údaje

Správce musí přijmout s ohledem na povahu, rozsah a účely zpracování vhodná technická a organizační opatření, aby zajistil nejenom bezpečnost, ale také aby byl schopen doložit, že zpracování je prováděno v soulasu s GDPR. Správné zabezpečení slouží jako prevence k možnému úniku dat a k porušení povinností vyplývajících z právních předpisů. Čl. 32 hovoří o přijetí opatření velmi obecně a nezmiňuje konkrétní opatření. Každý zaměstnavatel by tak měl zvolit adekvátní možnost, jak údaje chránit. Pokud jsou osobní údaje obsaženy v listinné podobě, může se jednat o vhodně vedené evidence, uzamykatelné schránky a omezený počet oprávněných osob, které budou mít k údajům přístup. Dopad takových opatření můžeme vidět i v tom, že osobní spisy zaměstnanců by neměly být volně přístupné, což vyplývá i z § 312 odst. 2 ZP, který stanovuje oprávněné osoby, které by měli mít ke spisu přístup. V případě elektronických dat, je základem vhodné zálohování dat, využívání pseudonymizaci anebo šifrování osobních údajů. Volba konkrétních

¹⁰⁶ 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. a recitál č. 39 GDPR

¹⁰⁷ VLACHOVÁ, Barbora. Zákon o zpracování osobních údajů: komentář. V Praze: C.H. Beck, 2019. Beckovy komentáře. ISBN 978-80-7400-760-6, s. 19.

opatření bude vždy záviset na uvážení zaměstnavatele jako správce s přihlédnutím na konkrétní podmínky a technické možnosti.¹⁰⁸

3.1.4. Ohlašovací povinnost

Pokud dojde k porušení zabezpečení osobních údajů, musí správce toto porušení bez zbytného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu.¹⁰⁹ Dle čl. 4 odst. 12 GDPR porušení znamená „porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.“¹¹⁰

V oznámení musí správce popsat povahu porušení, přijatá opatření a pravděpodobné důsledky. Pokud dojde k porušení u zpracovatele, tak ten nejdříve obeznámí s touto skutečností správce a ten následně ÚOOÚ.

Pro další postup ÚOOÚ je stěžejní, zdali a jaká opatření k zabezpečení osobních údajů správce přijal před vznikem incidentu, a jaká opatření učinil k nápravě, resp. k minimalizaci nežádoucích účinků bezprostředně po zjištění porušení zabezpečení. To znamená ještě před jeho ohlášením Úřadu. Vhodným preventivním opatřením je např. zaheslování elektronických dokumentů obsahujících osobní údaje, zálohování evidencí s osobními údaji anebo pravidelná školení osob, které mají pravidelný přístup k osobním údajům.¹¹¹

Ohlašovat není třeba případy, u nichž je nepravděpodobné, že by porušení mělo za následek riziko pro dotčené osoby. Může jít např. o momentální nemožnost dohledat listinný dokument v manuálně vedené evidenci (kartotéky) fyzických osob, přičemž je nepravděpodobné, že by se dostal do nepovolanych rukou. Veškeré případy porušení zabezpečení osobních údajů (takže i ty, které nepodléhají povinnosti ohlášení) je však správce povinen dokumentovat.¹¹²

¹⁰⁸ KORNEL, Martin. KMOŠKOVÁ, Jitka. Povinnosti zaměstnavatele při ochraně osobních údajů zaměstnanců dle GDPR. Personální a sociálně právní kartotéka. Praha: Wolters Kluwer, 2017, roč. 20, č. 11, s. 7-13

¹⁰⁹ čl. 33 GDPR

¹¹⁰ čl. 4 odst. 12

¹¹¹ Porušení zabezpečení osobních údajů. Úřad pro ochranu osobních údajů. Dostupné z: <https://uoou.gov.cz/profesional/poruseni-zabezpeceni-osobnich-udaju>

¹¹² Základní příručka k ochraně údajů: Obecné nařízení. In: Uoou.cz [online]. Dostupné z: <https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju>

Při určování rizika porušení zabezpečení bude nutné vycházet zejména z kategorie osobních údajů, které byly porušením zabezpečení dotčeny. Vyšší riziko budou vždy představovat zvláštní kategorie osobních údajů (např. údaje o zdravotním stavu), případně údaje, jimiž lze způsobit subjektu údajů závažnou újmu či zásah do jeho práv (např. únik přihlašovacích údajů do elektronického bankovníctví). Dalším rozhodným prvkem může být i okolnost, zdali došlo k porušení zabezpečení úmyslně či nedbalostně, přičemž úmyslný čin výrazně zvyšuje riziko takového činu, jelikož osobní údaje byly terčem útoku. Určení rizika porušení zabezpečení se tak musí provést komplexně, nikoli izolovaně a vyšlé riziko následně určí eventuální povinnost oznámit porušení zabezpečení Úřadu pro ochranu osobních údajů nebo i oznámit subjektu údajů.¹¹³

3.2. Práva subjektu

Povinnostem správce, coby zaměstnavatele odpovídají práva zaměstnanců, která jsou obsažena v čl. 13 až 22 GDPR. Konkrétně se jedná o právo na přístup k osobním údajům, právo na opravu, právo na výmaz, právo na omezení zpracování, právo na přenositelnost a právo podat námitky. V literatuře se můžeme setkat s tím, že informační povinnost zaměstnavatele je vyjádřena jako právo na informace na straně zaměstnance. Pro systematiku práce se autorka přiklonila k tomu, že informování subjektu je povinností zaměstnavatele, neboť je to jediné právo, které je pasivní. Ostatní práva v čl. 15 až 22 GDPR jsou práva aktivní. Práva subjektů v podstatě zrcadlově odpovídají povinnostem správce, ale subjekt o ně musí požádat, anebo jinak informovat správce, aby toto právo mohlo být naplněno.¹¹⁴

Výčet těchto práv není konečný, v čl. 77 odst. 1 GDPR je právo subjektu podat stížnost u dozorového úřadu, pokud se subjekt domnívá, že zpracování probíhá v rozporu s GDPR a došlo k porušení jeho práv. V čl. 82 odst. 1 GDPR je poté přiznává subjektu právo na náhradu újmy v případě, kdy bude rozhodnuto v jeho prospěch.¹¹⁵

¹¹³ Základní příručka k ochraně údajů: Obecné nařízení. In: Uoou.cz [online]. Dostupné z: <https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju>

¹¹⁴ JANEČKOVÁ, Eva. GDPR: praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. str. 16-25

¹¹⁵ Čl. 77 a 82 GDPR

3.2.1. Právo na přístup k osobním údajům

Toto právo je upraveno čl. 15 GDPR a jeho obsahem je právo subjektu získat od správce potvrzení, zda osobní údaje, které se ho týkají jsou nebo nejsou zpracovávány. Pokud je odpověď na tuto otázku kladná, může subjekt požadovat další informace o zpracování, a to např:

- Účel zpracování
- Kategorii dotčených osobních údajů
- Kategorie příjemců, kteří mají k osobním údajům přístup
- Doba, po kterou budou údaje zpracovávány
- Požadovat právo na opravu nebo výmaz
- Právo vznést námitky a podat stížnost proti zpracování
- Veškeré informace dostupné o zdroji osobních údajů, pokud nejsou získány od subjektu údajů.¹¹⁶

Na rozdíl od informační povinnosti je právo na přístup k osobním údajům právem aktivním ze strany subjektu, tudíž bez podání žádosti nemusí správce činit žádné kroky.¹¹⁷

K uplatnění tohoto práva poskytne správce na žádost o bezplatné poskytnutí kopie všech zpracovávaných údajů o daném subjektu. V kopii může být více údajů, než které sám subjekt poskytl, obsahem mohou být i záznamy z bezpečnostních kamer nebo záznamy telefonických hovorů. Žádost může subjekt podat i opakovaně, ale nesmí se z jeho strany jednat o nepřiměřené množství žádostí, za účelem šikanózního chování směrem k zaměstnavateli. Tomu dává čl. 12 odst. 5 GDPR obranné mechanismy proti nepřiměřenému a nedůvodnému podávání žádostí, kterými jsou právo účtovat přiměřený poplatek na základě administrativních nákladů anebo žádost odmítnout.¹¹⁸

3.2.2. Právo na opravu

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. Opět se jedná o aktivní právo na straně

¹¹⁶ ZEMANOVÁ ŠIMONOVÁ, Hana. Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů. Bulletin advokacie, č. 9/2017, Dostupné z: <http://www.bulletin-advokacie.cz/reforma-ochrany-osobnich-udaju-v-eu-z-pohledu-pracovnepravnich-vztahu>

¹¹⁷ GREPL, J. Kapitola V. Subjekty údajů. In: FIALA, GREPL, LICHNOVSKÝ 2019 op. cit., str. 98-107

¹¹⁸ Čl. 12 odst. 5 GDPR

subjektu, který požádá o opravu nepřesných údajů a dle čl. 18 odst. 1 písm. a) GDPR má právo na to, aby správce omezil jejich zpracovávání do doby, než ověří jejich přesnost. Subjekt může požadovat, aby neúplné údaje byly doplněny, případně aktualizovány dle potřeby. V případě uplatnění tohoto práva je správce povinen oznámit jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy, které učinil, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí.¹¹⁹

3.2.3. Právo na výmaz

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají. Nejedná se o právo absolutní, takže ne vždy může být žádosti zaměstnance vyhověno. Limity tohoto práva obsahuje čl. 17 GDPR, ve kterém jsou uvedeny důvody, pro které má správce povinnost osobní údaje bez zbytečného odkladu vymazat. Tyto důvody se neuplatní, pokud je zpracování nezbytné dle čl. 17 odst. 3, které zakládá další právní důvody pro zpracování, jako je splnění povinností ze zákona.

V souladu se zásadou zákonnosti odpovídá správce za správný způsob likvidace. Může ji provést úplnou anonymizací údajů anebo jejich fyzickým zničením, pokud jsou v listinné podobě. Pokud jsou v elektronické podobě, je taktéž možné je upravit, aby osoba nemohla být identifikována. V případě kamerových záznamů tak může jít o rozmazání obrazu, v případě zvukového záznamu lze změnit hladinu hlasu. Tento postup se uplatní, pokud např. na videozáznamu není osoba samotná, ale je jich tam více a záznam se uchová kvůli údajům těchto osob, pokud by se však záznam týkal jen této osoby, pak je lepším přístupem jeho úplné odstranění.

3.2.4. Právo na omezení zpracování

Toto další aktivní právo souvisí s právem na výmaz osobních údajů, ale na rozdíl od práva na výmaz se jedná o právo dočasné. Uplatní se především v situacích, kdy nejsou naplněny důvody pro výmaz osobních údajů, anebo je úplné smazání pro subjekt údajů neúčelné.¹²⁰ Právo na omezené zpracování se uplatní

¹¹⁹ JANEČKOVÁ, Eva. GDPR: praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. str. 3-9

¹²⁰ RÁMIŠ, V. Článek 18. In: UŘIČAŘ, M. Obecné nařízení o ochraně osobních údajů: komentář. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.

např. v případě, kdy nejsou údaje přesné a na dobu potřebnou k jejich úpravě se omezí jejich zpracovávání. Další důvody jsou vymezeny v čl. 18 odst. 1 GDPR.

Jedním z možných způsobů, jak omezit zpracování údajů je přesunutí do jiného systému zpracování, znepřístupnění vybraných údajů uživatelům nebo v případě elektronických zdrojů je dočasně stáhnout např. z internetových stránek správce. Pokud se žádost vztahuje na automatizované zpracování, mělo by být omezení zajištěno technickými prostředky tak, aby se na osobní údaje nevztahovaly žádné další operace. Běžná lhůta omezení činí 1 měsíc, ale může být podle potřeby prodloužena.¹²¹

3.2.5. Právo na přenositelnost údajů

Toto právo lze využít pouze v případě, kdy se jedná o zpracování osobních údajů na základě souhlasu anebo založeného smlouvou, kdy je zpracování prováděno automatizovaně. Po žádosti má subjekt možnost získat od správce osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu. Tyto údaje pak může bez omezení předat jinému správci, případně může požadovat, aby předání inicioval sám správce, je-li to technicky proveditelné.

Výkonem práva na přenositelnost však nesmí být nepříznivě dotčena práva a svobody jiných osob. Účelem tohoto práva bylo posílení pozice subjektu údajů, kteří tak mohou snadněji nakládat se svými údaji.¹²²

3.2.6. Právo vznést námitku

Pokud správce provádí zpracování osobních údajů na základě svých oprávněných zájmů anebo kvůli nezbytnosti pro splnění úkolu prováděného ve veřejném zájmu, má subjekt podle čl. 21 GDPR právo vznést námitku proti zpracování údajů, které se ho týkají. Zaměstnanec tak může vznést námitku proti takovému zpracování, pokud má pochybnost, zda je v konkrétní věci skutečně přítomen onen oprávněný zájem zaměstnavatele. Ten tedy musí prokázat, na základě výsledku balančního testu, že zpracovává údaje oprávněně a jeho zájmy převažují právo na soukromí na straně zaměstnance. Zaměstnavatel by se měl držet

¹²¹ JANEČKOVÁ, Eva. GDPR: praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. str. 15-19

¹²² Stanovisko WP 29 (WP 242) ze dne 13. 12. 2016, revidované a přijaté dne 5. dubna 2017 pokyny týkající se práva na přenositelnost údajů.

zásady minimalizace osobních údajů a zbytečně nezpracovávat osobní údaje, které nejsou třeba pro naplnění stanoveného účelu.¹²³

Pokud je subjekt se svojí námitkou úspěšný, vzniká mu právo na výmaz dle čl. 17 odst. 1 písm. a) GDPR.

3.2.7. Právo nebýt předmětem rozhodování založeného na automatizovaném zpracování osobních údajů

Poslední aktivní právo, které uzavírá katalog práv subjektů, je právo nebýt předmětem automatizovaného individuálního zpracování upravené v čl. 22 GDPR. Toto právo zajišťuje subjektu údajů, že nebude předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky. Automatizované rozhodování je přípustné v případě, kdy je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem, anebo je takové rozhodnutí založeno na výslovném souhlasu subjektu údajů.¹²⁴

¹²³ GREPL, J. Kapitola V. Subjekty údajů. In: FIALA, GREPL, LICHNOVSKÝ 2019 op. cit., str. 98-107

¹²⁴ Rücklová, J. B. K. (2018, July 18). Jaká jsou Vaše práva v souvislosti s ochranou osobních údajů? Právní prostor. Dostupné z: <https://www.pravniprostor.cz/clanky/ostatni-pravo/jaka-jsou-vase-prava-v-souvislosti-s-ochranou-osobnich-udaju>

4. Ochrana osobních údajů v jednotlivých fázích pracovního poměru

V rámci předchozích kapitol byly představeny jednotlivé pojmy, zásady a vzájemná práva a povinnosti obou stran, které musí být při práci s údaji dodržovány během všech fází pracovního poměru. Cílem této práce je výše uvedené zařadit do kontextu konkrétních situací, ke kterým dochází od okamžiku projevení zájmu uchazeče o pracovní pozici, po přistoupení k pracovní smlouvě a výkonu práce až do doby, kdy pracovní poměr končí.

Přestože k monitoringu dochází během výkonu práce a šlo by ho systematicky zařadit do předmětné kapitoly, bude mu věnována zvláštní pozornost v rámci samostatné kapitoly.

4.1. Ochrana před vznikem pracovního poměru

Již při náboru zaměstnanců dochází ze strany zaměstnavatele anebo jeho personálního oddělení ke zpracování značného množství osobních údajů uchazečů, kteří projeví zájem o danou pracovní pozici. Poměrně standardním případem je i situace, kdy jedinec z vlastní vůle zasílá svůj životopis potencionálním zaměstnavatelům, bez vypsání výběrového řízení. Pokud zaměstnavatel nemá o zaměstnance zájem, nestává se správcem jeho osobních údajů, jediné snad, že by uchazeč projevily zájem nechat se zařadit do databáze potencionálních uchazečů. V tomto případě se zaměstnavatel správcem stává, a to pouze pro účely potencionálního výběrového řízení a spravování této databáze.¹²⁵

V případě, kdy by měl zaměstnavatel o uchazeče zájem, ať už po zaslání životopisu anebo v případě, využití databáze, postupuje stejným způsobem, jako v případě vypsání řádného výběrového řízení.

Ještě před samotným vznikem pracovního poměru přichází zaměstnavatel do kontaktu se značným množstvím osobních údajů, neboť uchazeči posílají své životopisy, motivační dopisy a jiné podklady nezbytné k prokázání svých předpokladů a zkušeností. Zaměstnavatel osobní údaje získané z těchto dokumentů ukládá a stává se správcem, na kterého dopadají veškeré povinnosti s tím spojené.

¹²⁵ ŽŮREK, Jiří. GDPR v personalistice. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6, s. 116-119.

Základní právní rámec pro výběr uchazečů představuje § 30 odst. 1 ZP. Ten uvádí pravidlo, že zaměstnavatel smí po fyzické osobě vyžadovat pouze takové údaje, které mají bezprostřední souvislost s uzavřením pracovní smlouvy. Samotný výběr uchazeče je v plné kompetenci zaměstnavatele, je tedy v jeho dobrém zájmu získat co nejvíce informací, které mu zákon získat umožňuje. Kritéria nezbytná pro uzavření pracovní smlouvy lze vymezit jako hledisko kvalifikace, nezbytné požadavky pro výkon práce nebo zvláštní schopnosti. V předchozích kapitolách byly zmíněny nepřímé identifikátory, a právě ty můžeme vnímat, jako zvláštní schopnosti. Jedná se o charakterní znaky jedinců, spolehlivost, týmový duch, anebo příjemné vystupování, může zanechat na zaměstnavatele patřičný dojem a zcela určitě se jedná o informace podstatné k svobodnému a vážnému rozhodnutí zaměstnavatele.¹²⁶

Oproti informacím, které smí požadovat jsou v §316 odst. 4 demonstrativně obsaženy informace, které naopak požadovat nesmí. Tato úprava se sice vztahuje až na zaměstnance po podpisu pracovní smlouvy, ale pokud je zaměstnavatel nemůže požadovat po uzavření smlouvy, jen těžko bude odůvodnitelný důvod jejich zpracování před jejím uzavřením. Výčet zakázaných informací se částečně překrývá a doplňuje s výčtem uvedeném v §12 odst. 2 zákona o zaměstnanosti.¹²⁷

Během výběru uchazečů je zaměstnavatel také povinen dodržovat rovné zacházení a zákaz diskriminace. Tento požadavek vyplývá zejména z § 4 a §12 zákona o zaměstnanosti. Speciální úpravou k zákoníku práce je poté antidiskriminační zákon.¹²⁸

Po výběru vhodného uchazeče, odpadá právní důvod zpracování údajů neúspěšných uchazečů. Zaměstnavatel by tedy měl poskytnuté životopisy vrátit nebo zlikvidovat. Pokud si je chce ponechat pro budoucí použití, musí s tímto záměrem uchazeče obeznámit a získat souhlas, protože právní důvod zpracování pro účely smlouvy pominul a žádný jiný důvod nenastává, jako v případě úspěšných kandidátů, jejichž údaje smí dále zpracovávat pro účely plnění smlouvy. Druhou situací, kdy si může životopisy ponechat, je oprávněný zájem v případě

¹²⁶ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s 376-378

¹²⁷ tamtéž

¹²⁸ Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon)

potencionálního soudního sporu, z důvodu diskriminace, kdy je doba ponechání omezena na dobu příslušných promlčecích lhůt. Pod oprávněný zájem by se také mohla podřadit situace, kdy si nechá životopisy neúspěšných, po dobu, než uplyne zkušební lhůta přijatého, v tomto případě by musel odůvodnit, že se jedná o místo s vysokou fluktuací.¹²⁹

4.1.1. Uvedení nepravdivých informací uchazečem

Výše byly zmíněny informace, které zaměstnavatel může a které naopak nemůže vyžadovat. Co se ale stane, když uchazeč uvede nepravdivé informace? Pro posouzení této situace budeme vycházet z toho, že se jedná o údaje, které zaměstnavatel smí a je oprávněn požadovat. Neboť pokud by se jednalo o nelegitimní údaj, který není potřebný pro uzavření smlouvy, nebudou zde žádné právní důsledky, pokud uchazeč odpoví nepravdivě. Lhostejný je zde i úmysl uvést druhou stranu v omyl, neboť zaměstnavatel na tuto informaci zkrátka nemá žádné právo a jeho omyl ve skutečnosti, která nesouvisí s uzavřením pracovní smlouvy není právně významná.¹³⁰

V případě, kdy se jedná o informaci významnou pro uzavření pracovní smlouvy a zaměstnavatel je oprávněn ji zjišťovat, je nutné i zkoumat, zda byla nepravdivá informace sdělena omylem anebo úmyslně. Z hlediska právní úpravy omylu se musíme řídit ustanovením občanského zákoníku § 583 až §585 , podle kterého, pokud byl druhý uveden v omyl ohledně rozhodné okolnosti, činí se právní jednání neplatné. Zaměstnavatel je v takovém případě oprávněn se domáhat vypovězení pracovní smlouvy.¹³¹

4.1.2. LinkedIn, jako prostředek pro výběr uchazečů

Využívání sociálních sítí a online prostředí za účelem nábory zaměstnanců se stalo běžnou praxí. V současné době je největší personální síť LinkedIn, který se stal klíčovým nástrojem nejen pro jednotlivce hledající pracovní příležitosti, ale také pro zaměstnavatele a náborové specialisty při výběru zaměstnanců. Často se můžeme setkat s tím, že zaměstnavateli místo životopisu stačí odkaz na profil na

¹²⁹ 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.

¹³⁰ ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str 65-86

¹³¹ Rozsudek Nejvyššího soudu ČR ze dne 21. 5. 2015, sp. zn. 21 Cdo 2005/2014

LinkedInu, případně se může stát, že je sám uživatel na svém profilu osloven zaměstnavatelem.¹³²

Při náboru má zaměstnavatel k dispozici dva specifické účty, které mu usnadňují vyhledávání na základě klíčových slov. Díky těmto specializovaným účtům získávají náboráři lepší přístup k uživatelům a vidí i více informací např. o jaké typy pozic a úvazků mají zájem, pokud jsou vyplněné.¹³³

Uživatel může na LinkedInu sdílet v podstatě jakékoliv údaje. Povinné jsou pouze jméno, emailová adresa a mobilní číslo. Ostatní údaje, jako dosažené vzdělání, roky praxe, předchozí pracovní místa a další jsou dobrovolné. Ze strany zaměstnavatele samozřejmě mohou přijít obavy, zda jsou uvedené informace pravdivé. V pochybnostech může v rozsahu §30 odst. 2 ZP požadovat potvrzení dosaženého vzdělání, jazykových kurzů a dalších pracovních zkušeností. LinkedIn je stále jen nástrojem k tomu, aby došlo k prvnímu kontaktu mezi uchazečem a zaměstnavatelem. Po spojení ve většině případů proběhne osobní pohovor, kde má zaměstnavatel možnost se doptat na další podstatné informace. V případě, kdy zašle uživatel odkaz na svůj profil sám, se uplatní stejná pravidla, jako v případě, kdyby poslal listinný životopis s motivačním dopisem.

Po přihlášení je nutné, aby uživatel vyjádřil svůj souhlas s podmínkami užití sítě, které tvoří smlouva s uživatelem, zásady ochrany soukromí a zásady pro soubory cookies. Uživatel tak dává souhlas LinkedInu, aby se stal správcem jeho osobních údajů, které může dále publikovat a upravovat. Tento souhlas, ale není to samé, jako dovolení náborářům, aby ho mohli kontaktovat anebo zpracovávat jeho údaje.¹³⁴

Přestože je LinkedIn veden, jako pracovní síť a dalo by se předpokládat, že uživatelé budou skrz ni chtít získat práci, nemusí tomu tak nutně být. Profily na LinkedInu mohou mít stejný osobní charakter, jako je profil např. na Facebooku nebo Instagramu, neboť LinkedIn umožňuje navazování kontaktů s dalšími uživateli, sledování osobností, přidání se do skupin zaměřených na jednotlivé

¹³² LORENC, Jakub. Jak se daří jednotlivým sociálním sítím v České republice?. In: LinkedIn [online]. 25. 4. 2017 [cit. 16. 3. 2024]. Dostupné z: <https://cz.linkedin.com/pulse/jak-se-daří-jednotlivým-sociálním-sítím-v-české-republice-jakub-lorenc>

¹³³ Zásady ochrany soukromí. In: LinkedIn [online]. 11. 8. 2020 [cit. 16. 3. 2024]. Dostupné z: https://cz.linkedin.com/legal/privacy-policy?trk=hb_ft_priv

¹³⁴ Němeček, D. (2018, May 9). Vybrané aspekty sociální sítě LinkedIn ve světle | epravo.cz. EPRAVO.CZ. [cit. 18. 3. 2024] Dostupné z: <https://www.epravo.cz/top/clanky/vybrane-aspekty-socialni-site-linkedin-ve-svetle-gdpr-107540.html>

pracovní oblasti atd. Množství veřejných informací tedy může být relativně velké a jak uvádí WP29 ve svém stanovisku, samotná existence veřejně dostupného profilu není dostatečným důvodem pro zpracování zveřejněných údajů.¹³⁵

Dle GDPR je možné osobní údaje zpracovávat pouze na základě jednoho z šesti právních titulů v čl. 6 odst. 1. a ačkoliv jsou údaje na sociální síti veřejné a často je možné uživatele přímo kontaktovat, neznamená to, že je možné uživatele obesílat s veškerými sděleními. Prvotně by měl mít uživatel na svém profilu napsáno, že hledá nové pracovní příležitosti, čímž vyjadřuje svůj souhlas s kontaktováním. Pokud se v tomto ohledu nijak nevyjádřil, nicméně z jeho poskytnutých informací lze dovodit, že je možné jej takto kontaktovat může tak náborář učinit na základě titulu oprávněného zájmu dle čl. 6 odst. 1, písm. f) GDPR. Oprávněným zájmem zůstává nábor zaměstnance, a i obsah zpráv by se tak měl omezit na tuto tematiku. Uživatel by neměl být kontaktován za účelem marketingu, ani pozvánek na akce. Zaměstnavatel by měl také dbát na dodržení §30 odst. 2, kdy může získávat jen informace bezprostředně související s uzavřením pracovní smlouvy, čemuž odpovídá rovněž čl. 5 odst. 1 písm. c) GDPR, které ukládá správci povinnost zpracovat jen údaje, které jsou přiměřené, relevantní a omezené na nezbytný rozsah ke stanovenému účelu pro který jsou zpracovávány.¹³⁶

4.2. Ochrana při výkonu práce

Po vybrání úspěšného uchazeče a přistoupení k podpisu pracovní smlouvy, bude moct zaměstnavatel požadovat i další údaje, které během výběrového řízení nebyly relevantní. V této fázi pracovního poměru dojde ke shromáždění největšího množství informací a k jejich zpracování může zaměstnavatel v roli správce využít jakýkoliv z právních důvodů v čl. 6 GDPR. V praxi bude nejčastěji zpracovávat údaje pro účely plnění pracovní smlouvy dle čl. 6 odst. 1 písm. b) GDPR anebo pro plnění právních povinností, které se na správce vztahují dle čl. 6 odst. 1 písm. c).¹³⁷

¹³⁵ Stanovisko WP29 ze dne 8. června 2017 ke zpracování osobních údajů na pracovišti

¹³⁶ Němeček, D. Vybrané aspekty sociální sítě LinkedIn ve světle | epravo.cz. EPRAVO.CZ. [cit. 18. 3. 2024]. Dostupné z: <https://www.epravo.cz/top/clanky/vybrane-aspekty-socialni-site-linkedin-ve-svetle-gdpr-107540.html>

¹³⁷ Čl. 6 odst. 1 písm. b) a c) GDPR

Shromáždění těchto údajů vyplývá zaměstnavateli z ustanovení příslušných právních předpisů.¹³⁸ Z těchto zákonů můžeme vysledovat seznam údajů, které bude zaměstnavatel po novém zaměstnanci vyžadovat.

Jedná se o:

- Osobní údaje sloužící k přímé identifikaci zaměstnance, jako je jméno a příjmení, datum narození nebo místo trvalého pobytu. Tyto informace jsou často doplněny o rodná čísla anebo čísla občanských průkazů (ty jsou nutné například pro identifikaci zaměstnance u zdravotní pojišťovny anebo správy sociálního zabezpečení). Zaměstnavatel také může požadovat číslo řidičského průkazu, ale to jen v případě, kdy bude zaměstnanec řídit služební auto, v odlišných případech není právní titul pro tento údaj dostatečný.
- Údaje o nejvyšším dosažené vzdělání a roky praxe. Tyto údaje mohou být potřebné pro správný výpočet mzdy a platu.
- Pro správný výpočet měsíčních záloh na dani, je taktéž podstatné mít informace o pobíraných důchodech
- Informace o zdravotní pojišťovně pro placení zdravotního pojištění
- Státní občanství, kvůli hlášení cizinců
- Informace o zdravotním stavu, pro zjištění poměru zdravotně postižených zaměstnanců, pro splnění povinnosti zaměstnavatelů, kteří mají více než 25 zaměstnanců¹³⁹ a čerpání příslušných výhod¹⁴⁰
- Počet dětí u žen, pro zjištění přesného data vzniku nároku na odchod do starobního důchodu¹⁴¹

Pokud chce zaměstnavatel zpracovávat i jiné údaje než výše uvedené, může zpracování opřít o svůj oprávněný zájem dle čl. 6 odst. 1 písm. f). Takovým oprávněným zájmem může být zajištění bezpečnosti, zamezení podvodů anebo předávání osobních údajů v rámci skupiny podniků pro vnitřní administrativní

¹³⁸ zákoníku práce, zákonu o zaměstnanosti, zákonu o veřejném zdravotním pojištění i v zákonech z oblasti sociálního zabezpečení a dalších

¹³⁹ Pokud nejsou schopni zaměstnavatelé plnit povinný 4% podíl, poté musí odvádět ročně 2,5násobek průměrné mzdy.

¹⁴⁰ Zaměstnavatel má nárok na slevu na dani z příjmu, nižší mzdové náklady, nařízení vlády 567/2006 Sb.

¹⁴¹ Kontroly za rok 2007: Zaměstnavatel jako správce osobních údajů. In: Uoou.cz [online]. [cit. 20. 03. 2024]. Dostupné z: <https://www.uoou.cz/zamestnavatel-jako-spravce-osobnich-udaju/d6171/p1=5649>.

účely. Pro prokázání oprávněného zájmu je nutné provést tzv. balanční test, který posoudí, zda nejsou práva a zájmy subjektu přednější než oprávnění zaměstnavatele. Typickým příkladem takovýchto údajů je zpracování kontaktních údajů zaměstnance, jako je telefonní číslo anebo email. Ač jejich zpracování právní předpisy neukládají a nejsou nezbytné pro účely plnění smlouvy, ani nespádají pod povinnosti zaměstnavatele, je zde oprávněný zájem zaměstnavatele, který potřebuje zaměstnance kontaktovat, případně bude služební telefon sloužit k další komunikaci mezi zaměstnanci.¹⁴²

Třetí pomyslnou skupinu tvoří údaje, o kterých taktéž rozhoduje zaměstnavatel sám, ale v rámci balančního testu bude zpracování těchto údajů těžko obhajitelné. V tomto případě se jedná především o fotografie a zveřejnění podoby zaměstnanců ať už na webových stránkách anebo interních databázích. Vzhledem k tomu, že balanční test neobstojí, je nutné k těmto údajům mít souhlas zaměstnance. Tento souhlas musí být svobodný, konkrétní a jednoznačný, aby nedošlo k nejednoznačnému projevu vůle. Projevení souhlasu zaměstnance by však nemělo být běžnou praxí zaměstnavatele a taktéž v případě jeho neudělení by neměl následovat postih směrem k zaměstnanci. K souhlasu by se měl zaměstnavatel uchýlovat pouze v případech, kdy se nemůže opřít o jiné právní tituly. Odlišná bude situace v případě vedoucích zaměstnanců, u kterých by mohl oprávněný zájem obstát, neboť vedoucí by měl znát podobizny svých pracovníků a mohl by mít k dispozici interní databáze svých podřízených pracovníků.

§ 316 odst. 4 ZP udává taxativní seznam informace, které naopak zaměstnavatel nesmí zpracovávat. Jedná se o údaje, které nesouvisí s výkonem práce, informace, které by mohli vést k diskriminaci a taktéž z nich neplynou další právní nároky, jako např. v případě vzniku nároku na starobní důchod, anebo slevy na dani, vyplacení pojistného atd.¹⁴³ Přestože je jejich zpracování zakázáno, ZP stanovuje výjimky pro údaje o těhotenství, rodinných a majetkových poměrech a trestněprávní bezúhonnost, které mohou být zpracovány, pokud to spočívá v povaze práce a požadavek na jejich zpracování je oprávněný a přiměřený vzhledem

¹⁴² Mandát, J. Souhlas se zpracováním osobních údajů u zaměstnance | epravo.cz. EPRAVO.CZ. [cit. 20. 03. 2024]. Dostupné z: <https://www.epravo.cz/top/clanky/souhlas-se-zpracovanim-osobnich-udaju-u-zamestnancu-108010.html>

¹⁴³ MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR 2019. 420 s. ISBN 978-807598-587-3, s. 386

k povaze práce. Podmínky zpracování těchto údajů stanoví blíže zvláštní předpisy.¹⁴⁴

U výpisu z trestního rejstříku je však situace ještě komplikovanější, neboť záleží, jaký druh bezúhonnosti je vyžadován, jestli absolutní anebo ve vztahu k určitým trestným činům zásadním pro daný obor. V případě advokátů anebo soudců se jedná o absolutní zákaz, kdy se vyžaduje plná bezúhonnost včetně nedbalostních trestných činů. V případě pedagogických pracovníků je situace odlišná a postačí, pokud nespáchali trestnou činnost související s poskytovaným vzděláním. Přestože je prokázání trestné bezúhonnosti považováno za citlivý údaj, zaměstnavatel může vyžadovat výpis z rejstříku i v případě, kdy mu to neukládá zákon, jen je potřeba, aby právní důvod pro jeho zpracování byl oprávněný a přiměřený vzhledem k povaze práce. To trestní bezúhonnost staví mimo tradiční zvláštní údaje, u kterých se oprávněný zájem nemůže použít pro jejich zpracování. Stane se tak v případě, kdy zaměstnanec bude nakládat s finančními částkami anebo hodnotným zbožím, jako jsou šperky nebo elektronika, kdy v zájmu zaměstnavatele jistě je si ověřit bezúhonnost týkající se krádeže anebo zpronevěry. Pokud má uchazeč anebo zaměstnanec pochybnosti o potřebnosti těchto údajů, může podle zákona o zaměstnanosti požádat zaměstnavatele o prokázání potřebnosti požadovaných údajů. Pokud uchazeč anebo zaměstnanec nabude dojmu, že zaměstnavatel vyžaduje doložení bezúhonnosti v rozporu s právními předpisy, tak může podat stížnost na příslušný inspektorát práce.¹⁴⁵

4.2.1. Osobní spis zaměstnance

Veškeré dokumenty obsahující osobní údaje bývají zpravidla uloženy v osobním spisu zaměstnance. Ten slouží výhradně pro interní potřebu zaměstnavatele a pro řádný výkon práv a povinností v rámci pracovněprávního vztahu. Jeho úpravu najdeme v § 312 odst. 1 ZP a text zákona zní, že zaměstnavatel „je oprávněn“ ho vést. To může vyvolat pochybnosti o tom, zda se jedná o jeho libovůli anebo o povinnost. Vzhledem k tomu, že zaměstnavatel musí plnit své povinnosti a mít k dispozici velké množství dokumentů (jako je pracovní smlouva, dokumenty o kvalifikaci zaměstnance, osobní dotazníky, platové výměry,

¹⁴⁴ § 316 odst. 4 Zákonníku práce

¹⁴⁵ Kaletová, R. Lustrace zaměstnanců – kdy může zaměstnavatel chtít po zaměstnanci výpis z rejstříku trestů. Právní prostor. [cit. 20. 03. 2024]. Dostupné z: <https://www.pravniprostor.cz/clanky/pracovni-pravo/lustrace-zamestnancu-kdy-muze-zamestnavatel-chtit-po-zamestnanci-vypis-z-rejstriku-trestu>

podepsané BOZP, anebo souhlasy se zpracováním osobních údajů, podklady k prováděným srážkám, dokumenty o ukončení) lze předpokládat, že se skutečně jedná spíše o povinnost než o oprávnění.¹⁴⁶

Osobní spis už z logiky věci může obsahovat pouze písemnosti nezbytné pro výkon práce v základním pracovněprávních vztahu. V předchozím odstavci bylo naznačeno, o jaké dokumenty se může jednat, nicméně úplný výčet nikde stanoven není a taktéž není pravidlem, aby v rámci jednoho zaměstnavatele byly osobní spisy totožné, spíše je to více než nepravděpodobné a spisy jsou dosti diverzifikované. Proto je spíše dobré si vymezit osobní spis negativně a říct si, jaké dokumenty jeho obsahem být nemohou. Jedná se o informace a dokumenty, které zaměstnavatel nesmí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru¹⁴⁷ a dále informace nesouvisející s výkonem práce. Součástí osobního spisu by neměl být ani životopis, neboť jeho právní důvod pro zpracování končí poté, co je uchazeč přijat. Jeho přítomnost v osobním spisu je tak nadbytečná.¹⁴⁸

Vzhledem k tomu, kolik údajů osobní spisy obsahují, nemá k nim přístup kde kdo. Zaměstnavatel v postavení správce je povinen zajistit ochranu osobních údajů před neoprávněným přístupem nepovolaných osob nebo zneužitím. Do osobního spisu by měli mít možnost nahlédnout nejen kompetentní osoby podle § 312 odst. 2 ZP, ale také by zde měl být jasně stanovený důvod toho, proč do spisu nahlízejí. Aby se zamezilo tomu, že budou údaje poskytnuty nekompetentním osobám, je dobré si vést i záznamy o tom, kdo k osobnímu spisu přistupuje. Výčet osob není taxativní a přístup do spisu může mít i firemní právník, ředitel anebo statutární orgány zaměstnavatele. Jediná osoba, která do osobního spisu může nahlížet dá se říci neomezeně a nemusela by se kontrolovat, je sám zaměstnanec, který si může z osobního spisu činit výpisky a pořizovat stejnopisy na náklady zaměstnavatele a osobní spis by mu měl být, co nejvíce k dispozici, vzhledem k tomu, že se jedná o jeho údaje. Předmětný paragraf také uvádí, co se za nahlížení do spisu nepovažuje a jedná se o situace, kdy dochází ke kontrole vnějším orgánem, který si dokumenty z osobního spisu vyžádá.¹⁴⁹

¹⁴⁶ ZAHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 163

¹⁴⁷ §30 odst. 2 ZP

¹⁴⁸ §316 odst. 4 zákoníku práce

¹⁴⁹

4.2.2. Pořizování kopií dokladů

Jak již bylo rozebráno v první kapitole, rodné číslo nemusí být obsahem pracovní smlouvy. Zaměstnavatelé však často požadují při anebo krátce po podpisu pracovní smlouvy kopie různých dokladů, ať už je to kopie občanského průkazu, řidičského oprávnění anebo průkazu zdravotní pojišťovny. Pokud jde o občanské průkazy podle ustanovení § 15a odst. 2 zákona č. 328/1999 Sb. je zakázáno pořizovat kopie občanského průkazu bez prokazatelného souhlasu občana. Tento souhlas by měl splňovat náležitosti dle GDPR, což znamená, že by mělo být zřetelné, za jakým účelem je kopie pořizována a po jak dlouho dobu bude zaměstnavatel osobní údaje zpracovávat. Zaměstnavatel by neměl obecně pořizovat kopie dokladů svých zaměstnanců, pokud k tomu nesvědčí oprávněný právní důvod a on je nepotřebuje (viz u řidičského průkazu nutnost řídit služební auto). Pokud se tedy zaměstnavatel rozhodne kopie pořizovat, měl by tak činit v co nejmenším rozsahu a údaje uchovávat jen po omezenou dobu. Řešením by i bylo pořízení kopie s tím, že údaje, které nejsou potřeba zamaže.¹⁵⁰

K problematice kopií se vyjádřil i ÚOOÚ, který uvedl, že lepším postupem než pořizování kopií dokladů, je zaznamenání do osobního spisu, že dané doklady zaměstnanec předložil a do spisu se poznamená potvrzení, kdo a kdy na základě jakých dokladů je ověřil.¹⁵¹

4.2.3. Uveřejňování fotografií zaměstnanců

Po vzniku pracovního poměru může zaměstnavatel uchovávat fotografie zaměstnanců v osobním spise, v interní databázi na intranetu, může je umísťovat na nástěnky za účelem informování o absolvovaných školeních, teambuildingových akcích a podobně. Zaměstnavatel může také vytvořit zaměstnancům průkazky s jejich fotografií, které je v rámci společnosti identifikují.

Využívání fotografií zaměstnanců pro personální účely je během výkonu práce častou praxí, a přitom se jedná o povinnost, která zákoníkem práce není explicitně upravena. Kromě služebních průkazů, kde je fotografie požadována na základě zvláštní úpravy zákona o státní službě v § 154 odst. 1 písm. a), kdy služební

¹⁵⁰ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 95-100

¹⁵¹ Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2018. Praha: ÚOOÚ, 2019. str. 15.

průkaz musí fotografii obsahovat, je v ostatních případech zpracování fotografií povolené, jen v případě oprávněného zájmu.¹⁵²

Typickým příkladem je fotografie na vstupních kartách, která slouží jednak ke vstupu na pracoviště, tak k identifikaci. Užití fotografií na vstupních kartách anebo průkazkách může zajistit větší bezpečí zaměstnanců a taktéž majetku zaměstnavatele (vstupní karty s fotografií jsou často využívány v bankovních institucích, kvůli ochraně majetku). Ve velkých společnostech, kde se zaměstnanci navzájem neznají může být taktéž fotografie uvedena v interních seznamech. Oprávněným zájmem v tomto případě bude zajištění lepší komunikace mezi zaměstnanci. V takovýchto případech musí být zaměstnavatel schopen prokázat a dostatečně zdůvodnit oprávněný zájem. Pokud tento oprávněný zájem dostatečně neprokáže, měl by si zajistit souhlas zaměstnance. V případě internetové databáze, je oprávněný zájem relativně slabý, efektivní komunikaci lze zajistit i pomocí jména, oddělení a telefonního čísla, uvedení fotografií není nezbytně nutné. Obdobná situace nastane v případě pořizování a zveřejňování fotografií z konferencí anebo školení, na nichž lze osobu přímo identifikovat. Vzhledem k tomu, že má být souhlas zaměstnance dostatečně konkrétní a také by měl zaměstnanec vždy vědět, že k zveřejnění fotografií dojde, jeví se mi jako správný přístup při podpisu prezenční listiny, rovněž dodat listinu, která by obsahovala souhlas se zpracováním fotografií s uvedeným účelem. Pokud někteří z účastníků odmítnout své fotografie zveřejnit, musí být toto jejich právo vyslyšeno a zaměstnavatel by měl přijmout odpovídající opatření, spočívající v tom, že by ty, kteří souhlas nedali, usadil na jinou stranu místnosti. V žádném případě, nesmí být udělení nesouhlasu s pořizovanou fotografií na přítěž zaměstnanci.¹⁵³

Právní režim fotografií se řídí dle § 84 občanského zákoníku, který určuje, zda může a za jakých podmínek být zachycena podoba zaměstnance a jestli je potřeba mít jeho souhlas anebo lze využít zákonných podmínek, jako je tomu u služebních průkazů, kde tato povinnost fotografií poskytnou musí být splněna. Proto můžeme fotografie jako osobní údaje rozdělit na fotografie, které zaměstnavatel zpracovávat musí a které zpracovávat chce. V případě, kdy nebude

¹⁵² Zákon o státní službě

¹⁵³ ŽŮREK, Jiří. *GDPR v personalistice*. 2. doplněné vydání. Práce, mzdy, pojištění. Olomouc: ANAG, [2022]. ISBN 9788075543653.

z fotografie osoba rozpoznatelná, se nejedná o osobní údaj a ani o zásah do osobnostních práv.

4.3. Skončení pracovního poměru

Ať už skončí pracovní poměr dobrovolně z rozhodnutí zaměstnance, anebo nedobrovolně ze strany zaměstnavatele pro některý z výpovědních důvodů je nutné se vypořádat s osobními údaji a vydat potřebné dokumenty. S výjimkou, kdy zaměstnanec odchází do penze anebo pro jiný z důvodů přestane mít zájem o jakékoliv budoucí zaměstnání, má většina odcházejících zaměstnanců zájem, si co nejdříve najít zaměstnání nové. Na žádost odcházejícího zaměstnance, tak může zaměstnavatel vypracovat pracovní posudek.

Zákoník práce upravuje pracovní posudek ve větě druhé § 314 odst. 1, kdy se za pracovní posudek považují „*veškeré písemnosti, které se týkají hodnocení práce, kvalifikace, schopností a dalších skutečností, které mají vztah k výkonu práce*“ a zaměstnavatel je povinen vydat pracovní posudek do 15 dnů od žádosti zaměstnance, a to i v případě, kdy už ke skončení pracovního poměru došlo.¹⁵⁴ Zaměstnavatel není oprávněn uvádět nic nad rámec této definice, nicméně i tak, může být obsah posudku značně široký. Kromě výše uvedeného, může obsahovat i hodnocení celkového vztahu k práci, jako je svědomitost, dochvilnost, iniciativnost, pracovní kázeň, schopnost spolupráce v týmu atd. Svým obsahem, tak může představovat citelný zásah do ochrany osobnosti zaměstnance, i proto by měl být sepsán, co nejvíce objektivně a měl by vynechat subjektivní názory zaměstnavatele na vhodnost budoucího působení zaměstnance v určitém okruhu pracovních činností, komentáře k jeho soukromému životu či jiným činnostem, které nesouvisí s výkonem práce.¹⁵⁵

Napsat objektivní pracovní posudek je nelehký úkol a mohou nastat rozdílné situace. Posudek může vyznít značně negativně a v neprospěch zaměstnance, což není situace, o kterou by usiloval. V tomto případě se může vůči obsahu posudku bránit dle § 315 ZP žalobou u soudu a požadovat úpravu pracovního posudku. Cílem žaloby není vyhotovení nového, kladného posudku a zaměstnanec se tak nemůže u soudu bránit vždy, kdy se mu vyjádření zaměstnavatele nelíbí. V judikátu sp. zn. 21 Cdo 1362/2012 rozhodl Nejvyšší soud, že úprava posudku má být

¹⁵⁴ Rozhodnutí Nejvyššího soudu ČR ze dne 22. dubna 2003, sp. zn. 21 Cdo 1893/2002

¹⁵⁵ tamtéž

přiměřená a může k ní dojít jen v případě, kdy posudek obsahuje nepřiměřené subjektivní hodnocení, anebo údaje, které se nevztahují k výkonu práce.

Opačná situace může nastat, pokud je posudek napsán v přehnaných superlativech, které se nezakládají na pravdě. V takovéto situaci, kdy je zaměstnanec nepravdivě vychválen, však nedojde k žádné újmě ochrany jeho osobnosti a jediné, co zde hrozí je uvedení v omyl budoucího zaměstnavatele.

Na rozdíl od pracovního posudku, který je dobrovolný a vydává se na žádost, při odchodu zaměstnance musí zaměstnavatel vydat pracovní potvrzení § 313 ZP, které má své zákonem přesné vymezené obsahové náležitosti. Pokud by došlo k odchýlení, může zaměstnanec i v tomto případě podat žalobu, je, ale vhodné zmínit, že vzhledem k tomu, že jsou zákonem pevně dané obsahové záležitosti zaměstnavatel se nemá jak odchýlit, je rizikovost pracovního potvrzení mnohem menší.¹⁵⁶

Při skončení pracovního poměru je kromě vystavení potřebných dokumentů, také nutné přestat zpracovávat osobní údaje, jakmile uplyne poslední účel, který existuje pro jejich zpracování. Některé údaje by měly být zlikvidovány hned po ukončení vztahu, jiné až po uplynutí zákonné archivační doby či ponechány v případě oprávněného zájmu zaměstnavatele. Zaměstnavatel tak může nadále zpracovávat údaje bývalého zaměstnance, ale jen v omezeném rozsahu a po dobu, která je nezbytná k účelu jejich zpracování. Toto omezení vychází ze skutečnosti, že ačkoliv pracovní poměr zanikl, nedochází ve stejném okamžiku k zániku všech právních vztahů (např. vyplacení mzdy za poslední odpracované měsíční období).¹⁵⁷ Zpravidla se k dalšímu uchování využije jiný právní titul než pro účely plnění smlouvy, jak tomu bylo během výkonu pracovního poměru. Zaměstnavatel má např. povinnost ze zákona archivovat:¹⁵⁸

- Stejnopisy evidenčních listů důchodového pojištění – po dobu 3 let následujících po roce, kterého se týkají¹⁵⁹
- seznam společníků a členů statutárního orgánu a dozorčí rady u obchodní společnosti a záznamy o pojistném na sociálním zabezpečení a příspěvku na

¹⁵⁶ §315 zákoníku práce

¹⁵⁷ Rozhodnutí Úřadu pro ochranu osobních údajů č.j. SKO-2077/07. Úřad pro ochranu osobních údajů [online]. Úřad pro ochranu osobních údajů, © 2013 [cit. 15.03.2024]

¹⁵⁸ ZAHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 75-78

¹⁵⁹ Zákon č. 582/1991 Sb § 35a odst. 4 písm. d)

státní politiku zaměstnanosti – po dobu 6 let následujících po měsíci, kterého se záznam týká

- mzdové listy nebo účetní záznamy potřebné pro účely důchodového pojištění vedené pro poživatele starobního důchodu – 10 let, po roce, kterého se týkají
- mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění – 45 let, po roce, kterého se týkají¹⁶⁰

Zaměstnavatel, také může uchovávat dokumenty, které mu mohou posloužit v případě budoucích sporů např. o neplatnosti rozvázání pracovního poměru anebo při náhradě újmy. V případě, pokud by si potřebné údaje neuchoval, v případě sporu by byla jeho pozice značně oslabena. Obecně se doporučuje nechat si takovéto informace po celou dobu běhu promlčecích lhůt i krátce po nich, neboť žaloba může být žalovanému zaměstnavateli doručena i několik měsíců po uplynutí promlčecí lhůty. Z tohoto důvodu si může zaměstnavatel ponechat pracovnělékařské posudky, pro případné nároky zaměstnance na náhradu škody (při úrazu anebo nemoci z povolání). V případě těchto dokumentů lze doporučit lhůtu pro archivaci pracovnělékařských prohlídek minimálně po dobu 10 let od ukončení pracovního poměru, právě z důvodu případného uplatnění nároku na náhradu škody. Doba uchování těchto údajů je opět navázána na délku příslušné promlčecí lhůty.¹⁶¹

Z výše uvedeného je zřejmé, že není vhodné osobní spisy bývalých zaměstnanců ihned zrušit, ale zároveň není nutné je uchovávat v celém rozsahu. Dokumenty, kde není povinnost archivace a ty, u kterých neexistuje pravděpodobnost, že by je zaměstnavatel v budoucnu pro případný pracovněprávní spor se zaměstnancem potřeboval, je nutné okamžitě vyřadit. Mezi tyto dokumenty patří kopie osobních dokladů, profesní životopis anebo různá osvědčení. K výmazu osobních údajů musí dojít ve všech formách, a to jak fyzicky, tak v elektronické podobě, včetně vytvořených záloh. Po skončení pracovního poměru, by tak mělo dojít i ke stažení fotek zaměstnanců z webových stránek zaměstnavatele a zrušení pracovní emailové schránky. Pro případné vymáhání občanskoprávních nároků s největší pravděpodobností nebudou fotografie potřeba. Reportážní fotografie ze

¹⁶⁰ Zákon č. 582/1991 Sb § 35a odst. 4 písm. d) a §37 odst. 1 a 2

¹⁶¹ ZAHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 9788075023735. str. 75-78

zaměstnaneckých anebo jiných společenských akcí nicméně zůstat mohou, pokud zaměstnanec nedá najevo, že chce, aby byly odstraněny.¹⁶²

5. Monitoring zaměstnanců

V pracovním prostředí se monitoring jako proces sběru dat a informací využívá pro mnoho účelů. Zaměstnavatel může sledovat výkonnost a chování zaměstnanců pro zvýšení efektivity práce, zajištění bezpečnosti a zřejmě majoritním důvodem je ochrana jeho majetkových zájmů a preventivní zabránění zneužívání firemních prostředků.

Problematikou monitoringu je střet dvou zákonem garantovaných práv, a to právo zaměstnance na soukromí a oprávněné zájmy na straně zaměstnavatele a jeho právo na ochranu těchto zájmů. Pokud tedy zaměstnavatel chce sledovat své zaměstnance a jako důvod uvádí zajištění bezpečnosti, musí být tento jeho důvod silnější než právo zaměstnance na soukromí. Při střetu těchto dvou práv, by podle judikatury mělo mít soukromí, jako základní lidské právo, přednost, nicméně je třeba vždy pečlivě posoudit konkrétní okolnosti případu.¹⁶³ Z povahy pracovněprávního vztahu vyplývá, že je legitimní, aby zaměstnavatel kontroloval zaměstnance při užívání svěřeného majetku určeného k plnění pracovních úkolů a zaměstnanec je povinen mu sběr dat týkající se jeho osoby umožnit. Otázkou zde tedy není, zda zaměstnavatel může provádět monitoring, ale v jakém rozsahu tak může činit.¹⁶⁴

Kontrola a sledování zaměstnanců musí být vždy přiměřená vzhledem k účelu, pro který je zaváděna a zaměstnavatel musí dodržovat nejen GDPR, ale také zvláštní úpravu, kterou poskytuje zákoník práce v § 316 odst. 1 až 3. Pokud nějakou otázku zákoník práce neupravuje a jedná se současně o zpracování údajů, aplikují se právní normy GDPR anebo ZZOÚ. Podpůrnou právní úpravou jsou poté ustanovení občanského zákoníku, která se využijí vždy pokud se to týká ochrany osobnosti.¹⁶⁵

První odstavec daného paragrafu zakazuje zaměstnanci bez souhlasu zaměstnavatele užívat pro osobní potřebu výrobní a pracovní prostředky mu

¹⁶² 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.

¹⁶³ Městský soud v Praze ve svém rozsudku ze dne 30. 11. 2009, sp. zn. 11 Ca 298/2008

¹⁶⁴ Ustanovení § 2 a 38 zákona č. 262/2006 Sb.

¹⁶⁵ NONNEMANN, František. Soukromí na pracovišti. Právní rozhledy, 7/2015, s. 229-232 a násl.

svěřené. V souvislosti s § 301 písm. d) je tu také povinnost zaměstnance řádně s nimi hospodařit a chránit tím majetek zaměstnavatele. Spojení těchto dvou paragrafů uvádím, kvůli možnosti soukromého užívání po udělení souhlasu zaměstnavatele. Zaměstnanec musí o věci pečovat v jakémkoliv režimu, ať už soukromém nebo pracovním, a právě nedůsledné zacházení s prostředky může být důvodem pro odvolání souhlasu k soukromému užívání, případně podnětem k budoucí náhradě škody.¹⁶⁶

Souhlas zaměstnavatele nemá ze zákona určenou formu a může se jednat i o konkludentní ujednání, kdy zaměstnavatel toleruje dlouhodobé a vědomé soukromé používání. Za této situace je vyloučeno sankcionování zaměstnance, který jedná v dobré víře s tím, že mu zaměstnavatel mlčky souhlas poskytl, neboť k soukromému užívání nemá anebo neprojevuje žádné námitky. Zavedenou praxi může zaměstnavatel do budoucna změnit, neboť pravidla pro užívání pracovních a výrobních prostředků pro soukromé účely je zcela v jeho dikci. Pro doplnění je třeba uvést, že zaměstnavatel může žádat náhradu za soukromé užití, např. požadovat uhrazení ceny pohonných hmot.¹⁶⁷

V případě kontroly tohoto zákazu, se jedná o kontrolu nahodilou a krátkodobou, v ideální situaci vedenou bezprostředně vedoucími zaměstnanci.

Druhý odstavec § 316 se vztahuje na sledování zaměstnance, které probíhá dlouhodobě a systematicky. Zaměstnavatel k němu může přistoupit, pokud splní dvě podmínky. První z nich je existence závažného důvodu spočívajícího ve zvláštní povaze jeho činnosti. Závažným důvodem může být provoz, kde existují zvýšená rizika způsobení škody na zdraví i majetku (typicky se bude jednat o chemičky, čističky, jaderné provozy anebo banky a instituce nakládající s větším množstvím peněz atd.)¹⁶⁸ Závažný důvod se ale nemusí vztahovat jen na takto limitované zaměstnavatele, ale můžeme ho chápat i v širším slova smyslu, kdy legitimním důvodem pro sledování může být ochrana zaměstnanců a dalších osob, které se vyskytují v pracovním prostoru, ochrana majetku zaměstnavatele a kontrola pracovní výkonnosti. Druhou podmínkou je poté informativní povinnost směrem k zaměstnanci podle § 316 odst. 3. Samotné ustanovení nestanovuje, zda

¹⁶⁶ Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012

¹⁶⁷ PICHR T, Jan. Zákoník práce: Zákon o kolektivním vyjednávání. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-609-0.

¹⁶⁸ Rozsudek Nejvyššího správního soudu ze dne 20. 12. 2017, spis. zn. 10 As 245/2016 - 41

mají být zaměstnanci informováni před zahájením monitoringu, anebo stačí informování následně, nicméně kvůli ochraně zaměstnance, jako slabší strany by mělo jít o předchozí informace. Informativní povinnost lze vykládat různým způsobem, ideální forma je písemná dohoda mezi subjekty pracovního vztahu, nicméně např. u sledování pomocí kamer se jeví vhodným způsobem i přijmout opatření upozorňující na přítomnost kamer nepřetržitě, a to zvláště v případech, kdy do budovy zaměstnavatele vstupují i třetí osoby (v případech recepcí). Vhodným přístupem je umístění cedulek, které obsahují piktogram kamery anebo fotoaparátu.¹⁶⁹

O rozsahu, důvodu a konkrétní formě monitoringu rozhoduje zaměstnavatel bez toho, aniž by se musel poradit s další osobou, a i on je odpovědný za provedení balančního testu, který by se dal označit, jako třetí podmínka, kterou musí splnit. V rámci tohoto testu by měl zkoumat vhodnost, nezbytnost a přiměřenost jím zvoleného a nastaveného monitorovacího prostředku ve vztahu k vytyčenému účelu. V rámci testu by měl mimo jiné zjistit, zda účelu nemůže dosáhnout jiným, méně invazivním způsobem (např. místo zavedení kamer by stačila evidence pracovní doby. Pokud by kamery použil, jednalo by se o nepřiměřenou formu monitoringu).¹⁷⁰

Technický pokrok doby umožňuje zaměstnavatelům nespočet možností, jak zaměstnance sledovat, a to jak na pracovišti, tak v rámci homeoffice, jehož oblíbenost vzrostla během i po pandemii Covid-19. Nejčastější a také značně invazivní formu představují kamerové systémy. Další častou metodou, je sledování emailové korespondence, GPS lokátory, která slouží k zjištění polohy zaměstnance a kontrola aktivit zaměstnance na internetu. Zaměstnavatel ale může zajít i dále a existují programy, které detekují i pohyb myši na obrazovce nebo rychlost stisku kláves tkz. keylogger.¹⁷¹ V případě intenzivní kontroly zaměstnance musí mít zaměstnavatel důvodné podezření (např. páchání trestné činnosti) a zastřešovat vážný důvod, který by mohl ohrozit bezpečnost nejenom jeho a jeho zájmů, ale práv

¹⁶⁹ 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.

¹⁷⁰ K využívání testu proporcionality se vyjádřil Ústavní soud v nálezu ze dne 12. 10. 1994 se sp. zn. Pl. ÚS 4/94

¹⁷¹ Keylogger je druh programu, který snímá a zaznamenává stisky kláves na klávesnici.

třetích osob. Ve většině případů tedy bude využití obdobných intenzivních kontrol zaměstnanců nepřiměřené.

V rámci této kapitoly bych se chtěla věnovat běžným a v praxi nejčastěji využívaným formám monitoringu a dále možnostem zaměstnavatele kontrolovat zaměstnance na homeoffice, jehož oblíbenost a využívanost od pandemie Covid-19 roste.

5.1. Kamery na pracovišti

Z hlediska monitoringu a umístění kamer na pracovišti, je nejdříve nutné rozlišit, mezi kamerovým systémem bez záznamu a se záznamem.

Kamerový systém bez záznamu jen přenáší obraz z dané chvíle, bez toho, aby došlo k uložení a dalšímu nakládání s obrazem. Z tohoto důvodu tyto kamery nespádají pod ochranu ze strany GDPR, neboť za zpracování údajů se považuje až operace, která je prováděna se záznamem. Pokud je tedy kamerový systém pouze provozován, bez ukládání a šíření, nejedná se o zpracování osobních údajů.

V případě kamerového systému se záznamem, jak už název napovídá, dochází k uložení obrazového a případně i zvukového záznamu, za účelem pozdějšího využití těchto záběrů. Tím bude režim kamerového systému se záznamem přísnější, neboť zaměstnavatel se stává správcem údajů a dopadají na něj veškeré výše zmíněné povinnosti, které ve vztahu k monitoringu má. Nicméně je nutné podotknout, že i v tomto režimu nespadá každý záznam z kamer pod ochranu osobních údajů. Podle metodiky ÚOOÚ vydané v únoru 2024 je zpracováním osobních údajů, pokud postava v záběru zabírá 25% výšky obrazu, což je mezní obsah a při jeho aplikaci počítal ÚOOÚ i s úpravou obrazu, jako je zoom anebo jeho oddálení. Pokud tato mez není dosažena o osobní údaj se nejedná, neboť je zde předpoklad, že osoba zabírá tak málo obrazové plochy, že není rozpoznatelná.¹⁷²

Provozování kamer spadá pod §316 odst. 2, musí být tedy odůvodněno závažným důvodem spočívajícím ve zvláštní povaze činnosti zaměstnavatele, kdy zájem zaměstnavatele získat určité informace převáží právo na ochranu soukromí a osobnosti zaměstnance.

¹⁷² Nová metodika Úřadu ke kamerovým systémům. Úřad na ochranu osobních údajů. Dostupné z: <https://uoou.gov.cz/novinky/vse/nova-metodika-uradu-ke-kamerovym-systemum>

Problematickým je často samotné umístění kamer a prostoru, který snímají. V zákoně není explicitně uvedeno, která místa se nesmějí sledovat, nicméně máme zde účel, kvůli kterému jsou kamery instalovány, zásadu přiměřenosti a minimalizace zásahu do soukromí zaměstnanců, což některá místa rovnou vyčleňuje. Aby zaměstnavatel mohl dlouhodobě a systematicky sledovat zaměstnance ve společných prostorech (chodby, jídelny, místa k odpočinku) muselo by se jednat o výjimečnou situaci a nejspíše lepším řešením bude, pokud se umístění kamer v podobných prostorách vyhne. I kdyby měl zaměstnavatel podezření, že zaměstnanec odnáší z jídelny nádobí, zásah do soukromí zaměstnance bude převažovat nad zájmem na ochranu majetku zaměstnavatele. V případě toalet by byl zásah do soukromí zaměstnance velmi výrazný, takže zde se dá rovnou mluvit o téměř absolutním zákazu. Autorka schválně nechává prostor pro případné zcela mimořádné situace u zaměstnavatelů, jejichž činnost může být natolik specifická, jak ve vztahu k majetkovým hodnotám, anebo ke zdravotnímu riziku a bezpečnostním opatřením¹⁷³, kdy by mohl zájem zaměstnavatele převážít právo na soukromí a mohlo by dojít ke sledování i v těchto prostorách. Při běžném provozu se přiklání k zákazu využívání kamer v těchto místech.

Doba uložení záznamů není kogentně daná, ale obecně by neměl být kamerový záznam uložen déle, než je nezbytně nutné. V praxi se doba uchování pohybuje mezi 3 až 14 dny, s tím, že po 72 hodinách uchování by měl zaměstnavatel mít odůvodnění, proč nedošlo ke smazání.¹⁷⁴

Výše bylo uvedeno, že vůči zaměstnanci musí zaměstnavatel splnit informační povinnost. Co se ale stane, pokud tak neučiní a bude ho sledovat tzv. tajně? ESLP ve své judikatuře k čl. 8 Úmluvy sice stanovil podmínky tajného sledování, nicméně v podstatě nechává tuto oblast v působnosti vnitrostátní úpravy, která má určit možnosti i limity provádění tajného sledování. České právní předpisy mají řadu zákonů, které upravují různé formy tajného sledování např. trestní řád, zákony upravující fungování tajných služeb, zákon o Policii a další. Majoritu předpisů tvoří veřejnoprávní zákony spojené s trestním právem a sledování osob je zde zejména kvůli možnému riziku vzniku trestněprávní činnosti a k ochraně bezpečnosti. Žádný ze zákonů tak neupravuje vysloveně pracovníprávní oblast

¹⁷³ V případech, kdy by bylo ohroženo veřejné zdraví anebo hrozilo závažné bezpečnostní riziko

¹⁷⁴ Nová metodika Úřadu ke kamerovým systémům. Úřad na ochranu osobních údajů. Dostupné z: <https://uoou.gov.cz/novinky/vse/nova-metodika-uradu-ke-kamerovym-systemum>

k dané problematice. V §316 odst. 3 je uvedena informativní povinnost, kterou můžeme ve vztahu k tajnému sledování chápat jako odmítavý postoj, kdy tajné sledování ze strany zaměstnavatele je nepřípustné.¹⁷⁵

5.1.1. Použití falešných kamer

Případ, kdy zaměstnavatel používá falešné kamery je poměrně specifický. Z hlediska GDPR nepředstavují atrapy kamer žádný problém, protože z logiky věci nedochází ke zpracování osobních údajů, nicméně jejich instalace může být považována za porušení pracovněprávních předpisů. V tiskové zprávě z roku 2022 to uvedl i ÚOOÚ.¹⁷⁶ Ten v roce 2022 prověřoval podnět, který se týkal kamerového systému. Následně bylo zjištěno, že se jedná o falešné kamery, tudíž nešlo o osobní údaje a případ byl předán inspektorátu práce, který byl pro daný případ příslušný z důvodu, že nešlo o nakládání s osobními údaji. Ten konstatoval, že umístění falešných kamer může vytvářet na zaměstnance nepřiměřený tlak a jedná se o porušení povinností v § 302 písm. c) *vytvářet příznivé pracovní podmínky a zajišťovat bezpečnost a ochranu zdraví při práci.*¹⁷⁷

5.2. Elektronická pošta

Korespondenci zaměstnance můžeme rozdělit na klasickou v listinné podobě a vzhledem k pokroku doby v současné době častější elektronickou poštu. Ochrana listovního tajemství dopadá na oba uvedené způsoby komunikace a je uvedena v čl. 13 LZPS a stejný princip nenarušování obsahuje i § 182 trestního zákoníku. U tohoto způsobu kontroly, tak proti sobě stojí nejenom právo na soukromí, ale také právo na ochranu listovního tajemství, proti oprávněným zájmům zaměstnavatele, který může elektronickou poštu sledovat dle § 316 odst. 1 i 2 ZP.

Podle prvního odstavce může zaměstnavatel zakázat přijímání soukromých zpráv, neboť je zde předpoklad, že k přijetí soukromé zprávy se děje na svěřeném pracovním prostředku, a ten může zaměstnavatel z osobního využívání vyloučit.¹⁷⁸

¹⁷⁵ Evropský sbor pro ochranu osobních údajů. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [on-line]. Dostupné z: https://edpb.europa.eu/our-work-tools/ourdocuments/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 30-31.

¹⁷⁶ Atrapa kamery sice GDPR neporušuje, za její instalaci ale hrozí sankce - Česká justice. (n.d.). Česká justice. Dostupné z: <https://www.ceska-justice.cz/2022/05/atrapa-kamery-sice-gdpr-neporusuje-za-jeji-instalaci-ale-hrozi-sankce/>

¹⁷⁷ ZP § 302 písm. c)

¹⁷⁸ ZAHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 978-80-7502-373-5. str.163-169

Následný monitoring těchto soukromých zpráv pak má být omezen na jejich počet, nikoliv na obsah. Laicky řečeno, pokud má zaměstnavatel pocit, že zaměstnanec užívá email spíše jako soukromý než pracovní a porušuje tím zákaz zaměstnavatele, může provést kontrolu počtu těchto emailů (zhodnotit příchozí a odchozí zprávy, datový tok atd). Obsah soukromého emailu by mohl sledovat pouze v případě, že by z hlavičky emailu nerozpoznal, že jde o soukromou zprávu anebo pokud by jeho zájem převážil právo zaměstnance na soukromí. V tomto případě by se jednalo o kontrolu krátkodobou, z které by mohl okamžitě dovodit pro zaměstnance důsledky.¹⁷⁹

K pravidelnému sledování elektronické pošty by zaměstnavatel potřeboval závažný důvod dle §316 odst. 2. Tím v tomto případě může být plnění pracovních povinností zaměstnance, zda pravidelně komunikuje se zákazníky a dodržuje zásady firemní politiky v souvislosti správného jednání s klienty. I v tomto případě by měl kontrolovat je hlavičky emailů a neměl by se seznamovat s jejich obsahem. Nicméně, pokud by byl hrozilo utrpění jeho zájmů a bylo to nezbytné k ochraně jeho práv, po provedení balančního testu, kdy by to bylo nezbytné a přiměřené a zaměstnanec by byl informován, mohl by obsah soukromých emailů zaměstnavatel i číst. Zdržet by se měl tam, kde takový postup není nutný.¹⁸⁰

Existují výjimky, kdy zaměstnavatel může otevřít a vyřídit emailové zprávy doručené konkrétnímu zaměstnanci, a to zejména v zájmu ochrany svých práv, pokud je zřejmé, že nejde o soukromou zprávu anebo pokud je očekávání, že by zaměstnanec zprávu vyřídil pozdě a zaměstnavatel by došel k újmě. Tato situace může nastat v případě dlouhodobé nemoci zaměstnance.

5.3. Služební telefony a počítače

Služební telefony jsou společně s notebooky potažmo tablety nejvíce poskytovaným chytrým zařízením ze strany zaměstnavatele. Jelikož jsou tato zařízení pouze propůjčena, má zaměstnavatel zájem nejenom na jejich ochraně z hlediska majetkových práv a užívání jich v souladu s jeho pokyny, ale také chce, aby jejich užívání probíhalo, co možná nejefektivněji za účelem výkonu práce.¹⁸¹

¹⁷⁹ Doležal, R. (2021, Ma. Monitoring emailových zpráv zaměstnanců | epravo.cz. EPRAVO.CZ.Dostupné z: https://www.epravo.cz/top/clanky/monitoring-emailovych-zprav-zamestnancu-112690.html#_ftn7

¹⁸⁰ BARANCOVÁ, Helena, OLŠOVSKÁ, Andrea (eds.). Pracovní právo v digitalnej době. Praha: Leges, 2017. ISBN 978-80-7502-259-2, s. 164-165 a 168.

¹⁸¹ Rozhodnutí NS sp. zn. 21 Cdo 1771/2011.

Pokud mají zaměstnanci dovoleno používání telekomunikačních prostředků i k soukromým účelům, je monitoring pracovního telefonu prakticky vyloučen. A i v případě, kdy to dovoleno nemají, je vhodným řešením spíše napomenutí zaměstnance než přímé přistoupení k dlouhodobému monitoringu. Stejně jako v případě emailové korespondence, by měl zaměstnavatel kontrolovat spíše počet soukromých hovorů vzhledem k plnění pracovních povinností zaměstnance než jejich obsah. V obou případech se jedná o značně intenzivní zásah do soukromí zaměstnance.

Služební telefony často fungují na dvojím režimu, kdy je lze velmi snadno přepnout do pracovního anebo soukromého modu. Monitorování soukromých hovorů je nepřijatelné, stejně tak, jako jejich odposlouchávání. Zaměstnavatel tedy musí zajistit, aby v případě pracovních hovorů podléhal monitoring opět úpravě v § 316 odst. 2, který upravuje jak odposlech, tak záznam telefonických hovorů, které jsou typicky vedeny u call center anebo telefonních operátorů.¹⁸²

Pod služebním telefonem si nemusíme představit jen mobilní telefon, který má zaměstnanec u sebe, ale zahrnují se sem i pevné linky a obecná telefonní čísla, která jsou vázána např. na oddělení informací anebo recepci a nenáleží konkrétnímu zaměstnanci. V takovém případě může zaměstnavatel sledovat dobu trvání telefonu, jejich četnost, telefonní čísla volajících.¹⁸³

U pracovních počítačů je režim obdobný. Pokud dá zaměstnavatel souhlas podle §316 odst. 1, že může být počítač využíván i k soukromým aktivitám, případně se jedná o zavedenou praxi ve firmě, kdy zaměstnavatel neřeší soukromé využívání, je zřejmé, že nemůže vykonávat kontrolu nad způsobem využití služebního počítače. Situace by se mohla změnit, pokud by zaměstnanec nekonal svou práci anebo měl zaměstnavatel podezření, že dochází k porušování některého z interních předpisů. To by následně mohl konat kontrolu dle § 316 odst. 2, kdy by závažným důvodem byl zájem zaměstnavatele na ochranu např. obchodního tajemství anebo majetkových hodnot. V praxi je přísná kontrola ze strany

¹⁸² tamtéž

¹⁸³ VRBÍKOVÁ, B. Stanovisko Pracovní skupiny 29 k monitorování zaměstnanců na pracovišti i mimo něj. Epravo.cz. [online]. Publikováno 13. 9. 2017. [cit. 31. 3. 2022]. Dostupné z: <https://www.epravo.cz/top/clanky/stanovisko-pracovni-skupiny-29-k-monitorovani-zamestnancu-na-pracovisti-i-mimo-nej-106342.html>.

zaměstnavatele spíše nežádoucí, neboť podkopává důvěrný vztah mezi zaměstnancem a jeho nadřízeným.

5.4. GPS

Technologie GPS používají zaměstnavatelé zejména u svěřených automobilů či jiných dopravních prostředků. Nicméně i u propůjčené výpočetní techniky (telefony, počítače, tablety) je možnost zapnout sledování polohy. Ze získaných dat může zaměstnavatel zjistit nejen polohu zaměstnance, ale i trasu, po které se v rámci pracovního dne pohybuje a taktéž může dovodit další zaměstnancovi zvyklosti (např. kde tráví polední pauzu, kam chodí nakupovat anebo, jak řídí v případě, kdy systémy v autě reagují na náhlé brždění).¹⁸⁴

Právním titulem pro zpracování osobních údajů ze sledování bude oprávněný zájem zaměstnavatele. Dopravní prostředky nejsou levnou záležitostí a zaměstnavatel může požadovat jejich sledování za účelem ochrany majetkových práv. Dalším účelem může být zajištění bezpečnosti a ochrany zdraví při práci, dodržování pracovní doby a plnění odpočinkových přestávek.

Ze strany ÚOOÚ došlo k posouzení zákonnosti využití GPS k sledování zaměstnancům. Rozhodnutí ÚOOÚ ze dne 3. 7. 2013 se týkalo doručovatelů České pošty, kteří byli monitorováni GPS lokátorem, který po dobu jejich směny zaznamenával údaje o jejich geologické poloze. Česká pošta, tak sbírala údaje o pohybech doručovatelů, délce trasy a času stráveného na trase. Tento systém nazvali monitoring listovních zásilek a jeho účelem byla kontrola, sledování vytíženosti doručovaných okrsků a ochrana zaměstnanců před nerovnoměrným rozdělením práce.¹⁸⁵

Pokud bude využívat zaměstnanec vozidlo i k osobním účelům jedná se v podstatě o vstřícný krok zaměstnavatele a povinnosti směrem k vozidlu se budou řídit dohodou o použití tohoto vozidla. Při použití vozidla i na soukromé cesty by měla být možnost GPS lokátor vypnout a vyhnout se tak sledování. Nicméně ÚOOÚ se vyjádřil i k tomu, že pokud je to nutné, je možné automobil sledovat i pro soukromé účely, a to zejména kvůli plnění dalších zákonných povinností, jako je dodržení bezpečnostních přestávek nebo vedení evidence jízd, kterou je

¹⁸⁴ ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Teoretik. Praha: Leges, 2019. ISBN 978-80-7502-373-5. str191-200

¹⁸⁵ Rozhodnutí ÚOOÚ zn. INSP1-3568/12-16 ze dne 3. 1. 2013.

zaměstnavatel povinen vést k prokázání daňového uznání nákladů na pohonné hmoty.¹⁸⁶

Nejefektivnějším opatřením, které může zaměstnavatel k zajištění zákonnosti monitoringu zaujmout je možnost dočasného vypnutí sledovacího zařízení, které poskytne zaměstnanci potřebné soukromí na cesty nesouvisející s prací.¹⁸⁷

V souvislosti se sledováním aut je ještě nutné zdůraznit, že by stejně, jako u ostatních forem monitorování nemělo docházet k nadbytečnosti sledování.¹⁸⁸

5.5. Sledování aktivit zaměstnanců na internetu

S rostoucím využíváním informačních technologií v pracovním prostředí se objevuje stále větší potřeba sledovat, jak zaměstnanci využívají internetové zdroje a aplikace, které jsou běžnou součástí jim svěřených pracovních prostředků. K soukromému užívání propůjčené techniky potřebuje zaměstnanec souhlas a v situaci, kdy ho mít nebude, je zaměstnavatel oprávněn přiměřeně kontrolovat, zda je tento zákaz dodržován. Kromě výše uvedeného se může zaměstnavatel uchýlit k soustavnému sledování zaměstnance, jen za předpokladu existence závažného důvodu spočívající ve zvláštní povaze jeho činnosti. Tím může být podezření, že zaměstnanec neplní dostatečně své pracovní povinnosti anebo kvůli ochraně výpočetní techniky zaměstnavatele před škodlivými programy a viry. Zaměstnavatelé mohou používat speciální programy, které působí v podstatě na pozadí obrazovky a na rozdíl od kamer, nejsou na první pohled patrné a zaměstnanec o nich nemusí vůbec vědět.

Problematikou používání internetu je ten fakt, že použití přísného zákazu může být kontraproduktivní. Ne vždy se užívání internetu rovná zahálení. Zaměstnanci mohou využívat internet k dohledání informací souvisejících s pracovní činností a pokud zaměstnavatel sleduje jejich aktivitu na internetu pomocí programu nebo aplikace, měl by zároveň umět rozeznat, kdy zaměstnanec na internetu prokrastinuje, a kdy ho využívá pro práci. I z tohoto důvodu se liší přístup ÚOOÚ, inspekce práce i soudů k dané problematice, což nepříspěvá právní

¹⁸⁶ RADIČOVÁ, Zuzana. Monitoring zaměstnanců prostřednictvím GPS technologie. Právní rozhledy, 21/2014, s. 736 a násl.

¹⁸⁷ WP29, Stanovisko 2/2017 ke zpracování údajů na pracovišti, WP 249, 8. června 2017

¹⁸⁸ WP29, Stanovisko 5/2005 k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou, WP 115, 25. listopadu 2005

jistotě. ÚOOÚ vyžaduje přítomnost závažného důvodu a přiklání se spíše na stranu zaměstnance, kdy by zaměstnavatel neměl kontrolovat obsah ani dobu strávenou surfováním na internetu. Inspekce práce se ztotožňuje s vyjádřením ohledně obsahu, i ten pokládá za nepodstatný, nicméně dovoluje zaměstnavateli, aby sledoval i dobu strávenou zaměstnancem na internetu. Judikatura, která bude uvedena i níže, se poté přiklání k inspekci práce s tím, že přílišná doba používání internetu anebo Řešením by byla instalace softwaru, který umí následující rozpoznat a nedovolí zaměstnanci vstup na stránky, u kterých se dá předpokládat, že s pracovním výkonem nesouvisí. Vhodnou úpravou by bylo také použití vnitřního předpisu, který by povoloval využívání vyhledávačů, ale zakazoval využití určitých stránek, hraní her anebo sledování filmů v průběhu práce, kde se dá snadněji vyloučit, že by tyto aktivity souvisely s pracovní činností. Když zde využijeme názor WP29, zaměstnavatel má mít možnost zabránit zneužívání svěřených prostředků a sám technickými prostředky regulovat a předcházet tím konfliktním situacím. Zároveň, by ale takováto regulace neměla spočívat v úplném rozsahu. Vhodným opatřením je tak zákaz některých stránek, ale nechat možnost zaměstnanců užívat internetové vyhledávače. Zaměstnavatel stále musí volit takovou míru kontroly, která bude co nejméně zasahovat do soukromí zaměstnancům. Zpracování údajů by tak mělo být v rozsahu datum, hodina a délka přístupu na webové stránky a míra aktivity na nich.¹⁸⁹

Další stanovisko WP29 spočívá v tom, že by zaměstnavatel měl přistupovat ke kontrole okamžitě a nekumulovat zbytečně proti zaměstnanci důkazy. V tomto ohledu jistě záleží na chování zaměstnance, pokud je jednou upozorněn na prohřešek a ten se dále neopakuje, je skutečně zbytečné, uchovávat údaje o jeho webových aktivitách. Naopak, pokud nedochází ke zlepšení a zaměstnanec je v krátkém časovém období upozorněn vícekrát, pak je možné, aby zaměstnavatel záznamy uchovával, neboť tím chrání vlastní majetkové zájmy před zneužíváním ze strany zaměstnance.¹⁹⁰

Nejvyšší soud se věnoval aktivitě zaměstnance na internetu v rozhodnutí z roku 2012. V daném případě se zabýval žalobou zaměstnance, který chtěl zrušit

¹⁸⁹ Doležal, R., Cibulková, M., & Pomaizlová, K. (n.d.). Užití chytrých zařízení v pracovněprávních vztazích | epravo.cz. EPRAVO.CZ. Dostupné z: <https://www.epravo.cz/top/clanky/uziti-chytrych-zarizeni-v-pracovnepravnich-vztazich-a-ochrana-dat-112599.html>

¹⁹⁰ MORÁVEK, Jakub. Kdy je možné evidovat přístup zaměstnance na internet a otevřít jeho e-mailovou poštu? Právo pro podnikání a zaměstnání. 2010, roč. 19, č. 3, s. 7

neplatnost okamžitého zrušení pracovního poměru pro zvlášť hrubé porušení povinností dle § 55 odst. 1 písm. b) ZP. Zaměstnavatel odůvodnil tuto výpověď tím, že zaměstnanec hrubě porušil své povinnosti poté, co strávil více než 100 hodin své pracovní doby prohlížením internetových stránek, hraním her a vyřizováním soukromé korespondence. Zaměstnanec se bránil tím, že užití pro soukromé účely neprobíhalo na úkor plnění pracovních povinností a nenaplnila se tedy míra intenzivity zvlášť hrubého porušení a argumentoval také tím, že nebyl ze strany zaměstnavatele obeznámen se sledováním. Soud se přiklonil na stranu zaměstnavatele s tím, že rozsah soukromého užívání byl dostatečný k naplnění míry zvlášť hrubého porušení a navíc, zaměstnavatel nesledoval obsah internetových stránek, ale pouze dobu jejich užití. V daném případě v rozhodnutí soudu pomohlo právě i to, že měl zaměstnavatel stanovená pravidla ve vnitřním.¹⁹¹

Z rozsudku můžeme vysledovat dvě stěžejní věci k dané problematice. Prvním z nich je již zmiňovaná přítomnost vnitřního předpisu, která může vyjasnit, jak je to se zákazem využívání webových stránek ze strany zaměstnavatele myšleno a druhou je poté otázka, co by se stalo, kdyby zaměstnancova aktivita na internetu byla minimální a zda, by se dala tato činnost označit, jako předstírání práce, kdy dochází ke zneužívání majetku zaměstnavatele. Je jisté, že se musí vždy posuzovat okolnosti konkrétního případu, neboť pokud bude mít zaměstnanec své pracovní povinnosti splněné a udělanou i práci navíc a zaměstnavatel pro něho již nebude mít další, jak má pracovní dobu strávit? Nebude tato doba ideální k tomu, aby si směl vyřídit i své soukromé záležitosti? Dle autorky by to mělo být možné, pokud to nepostihne jeho pracovní výkon a bude to v přiměřeném rozsahu.

K méně závažnému využívání se vyjádřil Nejvyšší soud v rozhodnutí z roku 2014. I zde došlo ze strany zaměstnance k nepovolenému používání svěřené techniky (zde mobilního telefonu a počítače), zejména používání služebního telefonu pro soukromé účely. Co se týče vyhledávání informací na internetu, rozsah provinění nebyl takový, jako u předchozího rozhodnutí. Po obdržení výpovědi z důvodu soustavného méně závažného porušování pracovních povinností se obrátil zaměstnanec k soudu. Ve sporu šlo i o to, zda nebyla kontrola zaměstnance nepřiměřená a nenarušila zaměstnancova práva. Nejvyšší soud rozhodl obdobně, jako v předchozím rozsudku, kdy pokud se kontrola zaměřovala na množství času

¹⁹¹ srov. rozsudek Nejvyššího soudu ze dne 17. 10. 2012, sp. zn. 21 Cdo 2596/2011

stráveného používání internetu a ne obsahem prohlížených stránek, šlo o kontrolu přiměřenou.¹⁹²

5.6. Homeoffice

Homeoffice neboli práce na dálku je jednou z forem flexibilního zaměstnání, která je v současné době hojně využívána, přestože na tuto formu výkonu práce dlouho neměl zaměstnanec automaticky ze zákona nárok. Úpravu zákoníku práce přinesla novela č. 281/2023 Sb. s účinností od 1. 10. 2023. Předpis má dělenou účinnost, nicméně změny týkající se homeoffice platí již od října 2023., kdy nově mohou žádat o homeoffice lidé s dítětem mladším devíti let či pečující o blízké osoby. Nejedná se bohužel o automatický nárok ze zákona a zaměstnavatel může po odůvodnění písemně odmítnout. Novela zákoníku navíc neposkytuje konkrétní důvod, jak má vypadat zdůvodnění případného odmítnutí, což může vést i k výkladu, že v podstatě jakékoliv zdůvodnění je postačující. Takto nejasně vymezená hranice může vést i k případným soudním sporům.¹⁹³

Výkon práce na dálku je možný jen v případě písemné dohody mezi zaměstnavatelem a zaměstnancem. Co se týče legislativní úpravy, homeoffice není v žádném předpise výslovně zakotven. Částečnou úpravu můžeme najít v §317 ZP, který upravuje práci mimo pracoviště zaměstnavatele, která má být nadále vykonávána podle dohodnutých podmínek a v pracovní době, kterou si zaměstnanci rozvrhují sami. Práce na dálku je širším pojmem než práce z domova a bude aplikována na všechny případy, kdy se zaměstnanec se zaměstnavatelem dohodnout na výkonu práce mimo pracoviště.

Zaměstnavatel nicméně může určit nějaké omezení, např. určení určitého úseku hodin, kdy by měl být zaměstnanec přihlášený k práci a dostupný v rámci služebního telefonu. Dále je možné dojednat specifika rozvrhování dle typu práce zaměstnance. Pokud se kupř. konají periodické pracovní porady, je vhodné sjednat, aby zaměstnanec měl povinnost se těchto pracovních porad účastnit, a to prostřednictvím telefonu či videokonference.

I přestože pracuje zaměstnanec z domova, je možné, aby ho zaměstnavatel podrobil kontrole. Je, ale zřejmé, že charakter monitoringu bude v případě homeoffice odlišný. Jako první musíme uvést, ten fakt, že není možné kontrolovat

¹⁹² Rozsudek Nejvyššího soudu ze dne 7. 8. 2014, sp. zn. 21 Cdo 747/2013

¹⁹³ novela č. 281/2023 Sb, kterou se mění zákon č. 262/2006 Sb. zákoník práce

plnění pracovní doby, neboť ta je v kompetenci zaměstnance. Samozřejmě, může existovat dohoda mezi zaměstnavatelem a zaměstnancem ohledně hodin, kdy má zaměstnanec vykonávat práci, ale musíme vzít v potaz, že homeoffice má flexibilní pracovní dobu, která by neměla podléhat ze své povahy striktní kontrole. V rámci kontroly by si taktéž zaměstnavatel měl se zaměstnancem sjednat formu výsledků práce a kontrolu jejich kvality, neboť pracovní výsledky mohou být zřejmým ukazatelem, jak poctivě zaměstnanec pracuje. Zaměstnavatel také musí dohlížet na čerpání povinných přestávek.¹⁹⁴

Zaměstnavatel by neměl pro homeoffice nastavit mírnější ani přísnější režim, neboť nesmí dojít k diskriminaci a porušení rovného zacházení se všemi zaměstnanci. Pokud jsou zaměstnanci na pracovišti sledováni kamerami, anebo jejich docházka je monitorována pomocí čipových karet, měla by tu být stejná pravidla i pro zaměstnance na homeoffice, z důvodu zachování rovného zacházení. Čipové karty mohou sloužit i jako přihlašovací/ověřovací karty do služebních počítačů a taktéž mohou zaznamenávat pracovní doby systému, která by v podstatě odpovídala příchodu-odchodu. U kamerových záznamů je situace odlišnější, zejména kvůli citlivému prostředí. Pokud zaměstnanec vykonává práci doma, jsou prostředky monitoringu zaměstnavatele omezeny tím, že možnost narušení soukromí zaměstnance v momentě je větší. Kamery, by tak neměly zabírat celou jeho pracovní místnost, protože v podstatě prostory, kde pracuje a jejich vybavení, nespadá do údajů, na které by měl mít zaměstnanec právo.¹⁹⁵

¹⁹⁴ JANOTOVÁ, Magda. Home office v době koronaviru, jeho pravidla a dopady na ochranu osobních údajů. In: PaM profi - pracovní právo, mzdové účetnictví, personalistika [online]. Publikováno 6. 4. 2020 [cit. 25. 3.2024]

¹⁹⁵ JANOTOVÁ, Magda. Home office v době koronaviru, jeho pravidla a dopady na ochranu osobních údajů. In: PaM profi - pracovní právo, mzdové účetnictví, personalistika [online]. Publikováno 6. 4. 2020 [cit. 25. 3.2024]

Závěr

Problematika ochrany osobních údajů je velmi rozsáhlé téma. Autorka si tedy kladla za cíl poskytnout čtenáři komplexní náhled na danou problematiku, a ne detailní rozbor, neboť v rámci tématu by téma diplomové práce pokrylo i detailnější rozepsání jedné z kapitol. Cílem tak bylo seznámit čtenáře se základní pojmy a vývojem ochrany osobních údajů, která se byla dlouhou dobou jakousi podmnnožinou práva na soukromí, než se stala samostatnou oblastí. Od roku 2018 představuje právní rámec ochrany osobních údajů Obecné nařízení, známé jako GDPR, které nahradilo předchozí úpravu ve Směrnici 95/46/ES. Je jistě zajímavým poznatkem, že se nejednalo znovu o směrnici, ale o nařízení, které bylo bezprostředně použitelné v každém z členských států. Evropská unie tím potvrdila, jaký význam mají osobní údaje a jak potřebná je dostatečná míra jejich ochrany. GDPR sice umožňuje v čl. 88 stanovit konkrétnější pravidla k zajištění ochrany a soukromí, nicméně v ČR zatím nedošlo k přijetí žádných specifitějších pravidel. Nová úprava GDPR ani nezměnila definice a vzhledem k tomu, že jedním z jejích cílů bylo odstranění byrokratické zátěže, nedá se mluvit o úspěchu, protože naopak klade na správce a zpracovatele nové povinnosti na zabezpečení údajů. GDPR vzniklo proto, že Směrnice již nebyla aktuální a nezvládala reagovat na vývoj doby, je tedy otázkou, jak dlouho bude trvat, než se opět moderní technologie posunou o další level výše a vznikne nová právní úprava.

Vzhledem k tomu, že samotný vývoj ochrany osobních údajů je spjat s vývojem společnosti a její modernizací, snažila se autorka zvláště ve dvou posledních kapitolách věnovat i neustálé modernizaci technologií v rámci pracovního procesu, jak při výběru uchazečů a využívání online sociálního prostředí anebo při monitoringu během výkonu práce.

Moderní výpočetní technika jistě znamená velká ulehčení, mnoho procesů se automatizuje a přechází do online prostředí, ale nejen v pracovněprávních vztazích tím přibývají nové hrozby, na které musí právní oblasti reagovat.

Třetí kapitola byla věnována jednotlivým právům a povinnostem, ale také právnímu titulu souhlasu, jako jedné z možností na zpracování. Autorka zaujímá názor, že souhlas zaměstnance jako právní důvod ve většině případů až na výjimky není dostatečným důvodem k zpracování a zaměstnavatelé by vůči němu měli být velmi obezřetní. V rámci práce se autorka věnovala i nadbytečnému souhlasu a

teorii, jak moc je tento souhlas zaměstnance v případě nerovnosti stran a jeho podřízeného postavení svobodný.

Značná část práce byla věnována jednotlivým fázím pracovního poměr. Autorka se snažila vystihnout proces přijímání uchazečů, a to i se zapojením velmi oblíbené sociální platformy LinkedIn vyhledávání si informací ohledně uchazečů tímto způsobem.

V rámci poslední kapitoly se autorka věnovala formám monitoringu a to, jak na pracovišti, tak v případě práce z domova. Monitoring je oblastí, kde proti sobě stojí základní práva, a to právo na soukromí a právo na ochranu svého majetku. K monitoringu se zaměstnavatel může uchýlit, pokud mu k tomu svědčí závažný důvod spočívající v jeho zvláštní povaze, a právě tento podstatný pojem činí značný problém, neboť není doposud dostatečně vyložen. Kvůli neustálenému výkladu zde vzniká poměrně široký prostor pro právní nejistotu, i co se týká přijatých opatření, které zaměstnavatelé na ochranu svých garantovaných práv uplatňují.

Resume

This thesis examines the intricate landscape of data protection within employment relationships, focusing on the legal framework. In an era marked by increasing digitization and data-driven decision-making, it becomes imperative to address the balance between the employer's legitimate interests and the individual's right to privacy. 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 fourth 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.

With the proliferation of digital technologies, employers have increasingly turned to monitoring tools to supervise employee activities. However, this practice raises significant concerns regarding privacy, autonomy, and trust in the workplace. 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.

Klíčová slova

Osobní údaj, GDPR, soukromí, pracovní poměr, ochrana osobních údajů, zaměstnavatel a zaměstnanec

Keywords

Personal data, GDPR, privacy, employment relationship, personal data protection, employer and employee

Zdroje

Právní předpisy a mezinárodní smlouvy

1. 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
2. Smlouva o fungování Evropské unie
3. Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republik
4. 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
5. Zákon č. 262/2006 Sb., zákoník práce
6. Zákon č. 435/2004 Sb., o zaměstnanosti
7. Zákon č. 89/2012 Sb., občanský zákoník
8. Zákon č. 110/2019 Sb., o zpracování osobních údajů

Odborná literatura

1. BARANCOVÁ, Helena, OLŠOVSKÁ, Andrea (eds.). Pracovní právo v digitalnej době. Praha: Leges, 2017. ISBN 978-80-7502-259-2.
2. 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
3. JANEČKOVÁ, Eva. GDPR: praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1
4. MELOTÍKOVÁ, Petra. Ochrana osobních údajů v rámci veřejné správy. Praha: Leges, 2018. ISBN 978-80-7502-275-2.
5. MÍŠEK, Jakub. Moderní regulatorní metody ochrany osobních údajů. Brno: Masarykova univerzita, 2020. ISBN 978-80-210-9736-0.
6. 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.
7. NAVRÁTIL, Jirí a kol. GDPR pro praxi. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-689-7.
8. NONNEMANN, František. Příručka pověřence pro ochranu osobních údajů. Otevřeno. Praha: Klika, 2018. ISBN 978-80-88298-10-6.

9. 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.
10. PICHRT, Jan, a kol. Zákoník práce: Zákon o kolektivním vyjednávání. Praha: Wolters Kluwer, 2017. Praktický komentář. 1157 s. ISBN 978-80-7552-609-0. str. 918-92
11. ŠIMÍČEK, Vojtěch (ed.). Právo na soukromí. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3.
12. ŠTEFKO, Martin. Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochraně lidských práv a základních svobod. Jurisprudence. 2012, 21(7-8), 17-21. ISSN 1802-3843
13. RÁMIŠ, V. Článek 18. In: UŘIČAŘ, M. Obecné nařízení o ochraně osobních údajů: komentář. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.
14. ZAHRADNÍČEK, Jaroslav. *Ochrana osobnosti v pracovněprávních vztazích*. Teoretik. Praha: Leges, 2019. ISBN 978-80-7502-373-5.
15. ŽŮREK, Jiří. Praktický průvodce GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN: 978-80-7554-152-9. 19.
16. ŽŮREK, Jiří. GDPR v personalistice. Olomouc: ANAG, 2019. ISBN: 978-80-7554-210-6.

Elektronické zdroje

1. Doležal, R. (2021, Ma. Monitoring emailových zpráv zaměstnanců | epravo.cz. EPRAVO.CZ.Dostupné z: https://www.epravo.cz/top/clanky/monitoring-emailovych-zprav-zamestnancu-112690.html#_ftn7
2. Kaletová, R. Lustrace zaměstnanců – kdy může zaměstnavatel chtít po zaměstnanci výpis z rejstříku trestů. Právní prostor. [cit. 20. 03. 2024]. Dostupné z: <https://www.pravniprostor.cz/clanky/pracovni-pravo/lustrace-zamestnancu-kdy-muze-zamestnavatel-chtit-po-zamestnanci-vypis-z-rejstriku-trestu>
3. Mihulková, J.; Kornel, M. Co je, co není a co bude osobní údaj podle GDPR, 10. 2. 2018. Frank Bold Advokáti. (citováno dne 10. 3. 2024). Dostupné z:

<https://www.fbadvokati.cz/cs/clanky/541-co-je-co-neni-a-co-bude-osobni-udaj-podle-gdpr>

4. PRECLÍK, P. Šedesáté výročí Všeobecné deklarace lidských práv. em.muni.cz. (1. 2. 2009) Dostupné z: <https://www.em.muni.cz/udalosti/1325-sedesate-vyroci-vseobecne-deklarace-lidskych-prav> [cit. 18. března 2024]
5. NONNEMANN, F. Modernizace Úmluvy 108, základního nástroje Rady Evropy pro ochranu osobních údajů. In: Epravo.cz [online]. 20. července 2018. [cit. 13. března 2024]. Dostupné z: <https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html>
6. Šilhánková, I., & Hanák, J. (2021, únor 10). Nadbytečný souhlas se zpracováním osobních údajů | epravo.cz. EPRAVO.CZ. [cit. 11. 3. 2024] Dostupné z: <https://www.epravo.cz/top/clanky/nadbytecny-souhlas-se-zpracovanim-osobnich-udaju-v-pracovnepravnich-vztazich-jak-situaci-vyresit-112582.html>
7. LORENC, Jakub. Jak se daří jednotlivým sociálním sítí v České republice?. In: LinkedIn [online]. 25. 4. 2017 [cit. 16. 3. 2024]. Dostupné z: <https://cz.linkedin.com/pulse/jak-se-daří-jednotlivým-sociálním-sítí-v-české-republice-jakub-lorenc>
8. Němeček, D. Vybrané aspekty sociální sítě LinkedIn ve světle | epravo.cz. EPRAVO.CZ. [cit. 18. 3. 2024]. Dostupné z: <https://www.epravo.cz/top/clanky/vybrane-aspekty-socialni-site-linkedin-ve-svetle-gdpr-107540.html>
9. Rücklová, J. B. K. (2018, July 18). Jaká jsou Vaše práva v souvislosti s ochranou osobních údajů? Právní prostor. Dostupné z: <https://www.pravniprostor.cz/clanky/ostatni-pravo/jaka-jsou-vase-prava-v-souvislosti-s-ochranou-osobnich-udaju>
10. VRBÍKOVÁ, B. Stanovisko Pracovní skupiny 29 k monitorování zaměstnanců na pracovišti i mimo něj. Epravo.cz. [online]. Publikováno 13. 9. 2017. [cit. 31. 3. 2022]. Dostupné z: <https://www.epravo.cz/top/clanky/stanovisko-pracovni-skupiny-29-k-monitorovani-zamestnancu-na-pracovisti-i-mimo-nej-106342.html>
11. ZEMANOVÁ ŠIMONOVÁ, Hana. Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů. Bulletin advokacie, č. 9/2017, Dostupné z:

- <http://www.bulletin-advokacie.cz/reforma-ochrany-osobnich-udaju-v-eu-z-pohledu-pracovnepravnich-vztah>
12. Rozumné právo. Konec rodných čísel v občanských průkazech. Právní prostor. Dostupné z: <https://www.pravni prostor.cz/clanky/ostatni-pravo/konec-rodných-císel-v-obcanských-prukazech>
 13. Využívání zveřejněných osobních údajů | epravo.cz. (n.d.). EPRAVO.CZ. Dostupné z: <https://www.epravo.cz/top/clanky/vyuzivani-zverejnených-osobnich-udaju-109518.html>
 14. *Vše o OSN: historie, struktura, financování*. V Praze: Informační centrum OSN, c2014. ISBN 978-80-86348-18-6.
 15. Směrnice OECD o ochraně soukromí a přeshraničních tocích osobních údajů. [online]. 23. 9. 1980 [cit. 2024-03-18]. Dostupné z: <https://docplayer.cz/2620056-Prehled-smernice-oecd-o-ochrane-soukromi-a-preshranicnich-tocich-osobnich-udaju.html>
 16. Desatero omylů zpracování osobních údajů. ÚOOÚ [cit. 14. 3. 2024] Dostupné z: <https://uouu.gov.cz/verejnost/qa-otazky-a-odpovedi/desatero-omylu>
 17. Porušení zabezpečení osobních údajů. Úřad pro ochranu osobních údajů. Dostupné z: <https://uouu.gov.cz/profesional/poruseni-zabezpeceni-osobnich-udaju>
 18. Základní příručka k ochraně údajů: Obecné nařízení. In: Uoou.cz [online]. Dostupné z: <https://uouu.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju>
 19. Zásady ochrany soukromí. In: LinkedIn [online]. 11. 8. 2020 [cit. 16. 3. 2024]. Dostupné z: https://cz.linkedin.com/legal/privacy-policy?trk=hb_ft_priv
 20. Kontroly za rok 2007: Zaměstnavatel jako správce osobních údajů. In: Uoou.cz [online]. [cit. 20. 03. 2024]. Dostupné z: <https://www.uouu.cz/zamestnavatel-jako-spravce-osobnich-udaju/d6171/p1=5649>.
 21. Mandát, J. Souhlas se zpracováním osobních údajů u zaměstnance | epravo.cz. EPRAVO.CZ. [cit. 20. 03. 2024]. Dostupné z: <https://www.epravo.cz/top/clanky/souhlas-se-zpracovanim-osobnich-udaju-u-zamestnancu-108010.html>
 22. Atrapa kamery sice GDPR neporušuje, za její instalaci ale hrozí sankce - Česká justice. (n.d.). Česká justice. Dostupné z: <https://www.ceska->

justice.cz/2022/05/atrapa-kamery-sice-gdpr-neporusuje-za-jeji-instalaci-ale-hrozi-sankce/

23. Nová metodika Úřadu ke kamerovým systémům. Úřad na ochranu osobních údajů. Dostupné z: <https://uoou.gov.cz/novinky/vse/nova-metodika-uradu-ke-kamerovym-systemum>

Odborné články

1. MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad k § 316 ZPr. Právní rozhledy 17/2017. 8.
2. NONNEMANN, František. Soukromí na pracovišti. Právní rozhledy, 7/2015. 63 9.
3. RADÍČOVÁ, Zuzana. Monitoring zaměstnanců prostřednictvím GPS technologie. Právní rozhledy, 21/2014.
4. ŽŮREK, Jiří. K zákonu o zpracování osobních údajů. Praktická personalistika, č. 5-6/2019.

Judikatura

1. Nález Ústavního soudu ČR ze dne 1. 3. 2000 sp. zn. II. ÚS 517/99.
2. nález Ústavního soudu ze dne 9. 3. 2002 č. 299/2004 Sb.
3. 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.
4. nálezu ze dne 12. 10. 1994 se sp. zn. Pl. ÚS 4/94
5. Usnesení Ústavního soudu České republiky ze dne 5. září 2017, sp. zn. III. ÚS 3565/16.
6. Rozsudek Evropského soudu pro lidská práva ze dne 16. prosince 1992, stíž. č. 13710/88 ve věci Niemetz proti Německ
7. Rozsudek Nejvyššího soudu ČR ze dne 21. 5. 2015, sp. zn. 21 Cdo 2005/2011
8. Rozsudek Městského soudu v Praze ze dne 30. 11. 2009, sp. zn. 11 Ca 298/200
9. Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012
10. Rozsudek Nejvyššího správního soudu ze dne 20. 12. 2017, spis. zn. 10 As 245/2016 –14
11. Rozsudek Nejvyššího soudu ze dne 17. 10. 2012, sp. zn. 21 Cdo 2596/2011
12. Rozsudek Nejvyššího soudu ze dne 7. 8. 2014, sp. zn. 21 Cdo 747/2013
13. Rozsudek Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011.

Stanoviska a rozhodnutí ÚOOÚ a stanoviska WP 29

1. Stanovisko ÚOOÚ č. 3/2014, srpen 2014 k nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti.
2. Stanovisko ÚOOÚ č. 3/2009, revidované v červnu 2017 biometrická identifikace nebo autentizace zaměstnanců.
3. Stanovisko ÚOOÚ č. 3/2011: Ochrana osobních údajů podnikajících fyzických osob
4. Stanovisko ÚOOÚ č. 5/2013, říjen 2013 pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů
5. Stanovisko ÚOOÚ č. 3/2014. K nadbytečnému vyžadování souhlasu se zpracováním 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.