

Západočeská univerzita v Plzni

Fakulta právnická

GDPR v pracovním právu

Diplomová práce

Plzeň

Daniel Budil

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Daniel BUDIL
Osobní číslo:	R18M0029P
Studijní program:	M6805 Právo a právní věda
Studijní obor:	Právo
Téma práce:	GDPR v pracovním právu
Zadávací katedra:	Katedra pracovního práva a práva sociálního zabezpečení

Zásady pro vypracování

1. Úvod
2. Právní regulace GDPR
3. Základní pojmy a principy
4. GDPR v jednotlivých fázích pracovního poměru
5. Praktické otázky GDPR – monitoring zaměstnanců
6. Rozhodovací praxe Úřadu pro ochranu osobních údajů
7. Judikatura
8. Zahraniční exkurz
9. Závěr

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

Seznam doporučené literatury:

- BARTÍK, Václav, JANEČKOVÁ, Eva. Ochrana osobních údajů v aplikační praxi (vybrané problémy). 4. vyd. Praha: Wolters Kluwer ČR, 2016, 304 s. ISBN 978-80-7552-141-5.
- BARTÍK, Václav, JANEČKOVÁ, Eva. Ochrana osobních údajů v pracovním právu. (Otázky a odpovědi). 1. vyd. Praha: Wolters Kluwer, 2016, 192 s. ISBN 978-80-7552-145-3.
- MORÁVEK, Jakub. Ochrana osobních údajů v pracovněprávních vztazích. Praha: Wolters Kluwer ČR, 2013, 436 s. ISBN 978-80-7478-139-1.
- NEZMAR, Luděk. GDPR: Praktický průvodce implementací. 1. vyd. Praha: GRADA Publishing, 2017, 304 s. ISBN 980-80-271-0668-4.
- NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR, 2018, 580 s. ISBN 978-80-7598-068-7.
- Ochrana osobních údajů na pracovišti: příručka pro zaměstnance. Brno: Masarykova univerzita, 2014, 36 s. ISBN 978-80-210-6819-3.
- PICHRT, Jan a kol. Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář. Praha: Wolters Kluwer ČR, 2017, 1196 s. ISBN 978-80-7552-609-0.
- ŽÚREK, Jiří. Praktický průvodce GDPR. Olomouc: ANAG, 2017, 224 s. ISBN 978-80-7554-097-3.

Vedoucí diplomové práce: **JUDr. Martin Janák**
Katedra pracovního práva a práva sociálního
zabezpečení

Datum zadání diplomové práce: **1. února 2022**
Termín odevzdání diplomové práce: **31. března 2023**



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



Doc. JUDr. Jarmila Pavlátová, CSc.
vedoucí katedry

V Plzni dne 8. září 2022

Obsah

1	Úvod.....	8
2	Právní regulace GDPR	10
	2.1 Historie právní úpravy osobních údajů.....	10
	2.2 Předmět a cíle.....	13
	2.3 Věcná působnost	13
	2.4 Místní působnost	15
3	Základní pojmy a principy.....	17
	3.1 Osobní údaj.....	17
	3.2 Správce, zpracovatel.....	18
	3.3 Pověřenec pro ochranu osobních údajů.....	19
	3.4 Zpracování osobních údajů	22
	3.5 Omezení zpracování osobních údajů.....	23
	3.6 Zásada zákonnosti, korektnosti a transparentnosti	24
	3.7 Zásada minimalizace údajů	25
	3.8 Zásada přesnosti	25
4	GDPR v jednotlivých fázích pracovního poměru	25
	4.1 Zpracování osobních údajů před uzavřením pracovního poměru	26
	4.2 Zpracování osobních údajů za trvání pracovního poměru	27
	4.3 Zpracování osobních údajů po ukončení pracovního poměru....	32
5	Praktické otázky v souvislosti s GDPR – monitoring zaměstnanců	32
	5.1 Kamery na pracovišti.....	33
	5.2 Monitoring emailové pošty zaměstnanců.....	35
	5.3 Monitoring služebních telefonů.....	36
	5.4 Monitoring služebních automobilů	37
6	Rozhodovací praxe Úřadu pro ochranu osobních údajů	44
	6.1 Úkoly dozorového úřadu	46
	6.2 Pravomoci dozorového úřadu.....	47
7	Judikatura	55
8	Zahraniční exkurz	64
9	Závěr	66
	Cizojazyčné resumé.....	68
	Seznam použité literatury	71
	Knižní publikace.....	71

Internetové zdroje	71
Právní předpisy	72
Judikatura	73

Seznam ilustrací

Graf 1	Error! Bookmark not defined.
Graf 2	Error! Bookmark not defined.
Graf 3	Error! Bookmark not defined.
Graf 4	Error! Bookmark not defined.
Graf 5	Error! Bookmark not defined.

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

V Plzni dne 28.3.2023

Tímto bych chtěl poděkovat mému vedoucímu diplomové práce, JUDr. Martinu Janákovi za jeho odborné vedení, které přispělo k vypracování této práce.

1 Úvod

Od účinnosti evropského nařízení, které nese kompletní název Nařízení Evropského parlamentu a Rady č. 2016/679, obecně známého jako GDPR (General Data Protection Regulation), uběhlo již necelých 5 let. Osobní údaje začaly být diskutovaným a relevantním tématem, kterému se do příchodu GDPR nedávala taková pozornost. Cílem této diplomové práce bude komplexní rozbor a praktické dopady GDPR na situace v pracovním právu. Celkově bude tato práce rozdělena do třech částí a to na teoretickou, praktickou a judikaturní, aby čtenáři nabídla co nejširší spektrum fenoménu GDPR.

V první části, která zahrnuje kapitoly 2 a 3 bude věnován nejdříve prostor historickému kontextu a samotnému účelu GDPR, tedy odpovím na otázky, co vlastně zákonodárce vedlo k inovaci právního předpisu zabývajícího se ochranou osobních údajů. Kapitola 3 dále objasní nejvýznamnější pojmy, které problematika ochrany osobních údajů s sebou nese, a jejich pochopení je klíčové pro porozumění celého GDPR. Pojmy byly vybírány podle četnosti jejich běžného výskytu, tedy tak, že i čtenář, který se neflexibilně pohybuje ve sféře práva a problematice ochrany osobních údajů, bude seznámen s jejich významem. Dále zde bude brán zřetel i na stěžejní zásady obsahu GDPR, které lze označit stavebním kamenem struktury celého předpisu, a z jejichž linie se nelze odchýlit.

Druhá část bude tvořit samotné jádro diplomové práce, což lze vnímat jako praktické dopady GDPR na jednotlivé situace v pracovním právu. V kapitole 4 budou samostatně rozebírány stádia během pracovního poměru, tedy před, během a po ukončení. Tato kapitola má za cíl zaměstnanci objasnit, jakým způsobem může zaměstnavatel s jeho osobními údaji nakládat, a jak je zpracovávat během jednotlivých fází. Největší důraz bude kladen na časový interval během trvání pracovního poměru, neboť tento status vztahu mezi zaměstnavatelem a zaměstnancem lze označit za nejintenzivnější, a tedy bude i samotné zpracování osobních údajů nejfrekventovanější. V kapitole 5 budou řešeny reálné případy a situace na pracovišti s ohledem na zpracování osobních údajů zaměstnanců určitými prostředky. Budou rozebrány ty nejběžnější situace, kdy zaměstnavatel zpracovává osobní údaje zaměstnanců, ať už během pracovní

doby nebo mimo ní, a to skrz kamery, služební telefon nebo GPS lokátoru ve služebním automobilu. Cílem páté kapitoly bude vyložit čtenáři soulad tohoto zpracování osobních údajů s Nařízením, tedy vytyčit zaměstnavateli hranici zákonného zásahu do soukromí zaměstnance. Na to bude navazovat i dotazníkové šetření, u kterého bude vybráno několik praktických otázek, kdy budou respondenti, primárně zaměstnanci, odpovídat na situace v souvislosti s GDPR v pracovním právu. Výsledek jejich odpovědí bude zanalyzován, ve chvíli kdy zakomponuji zprvu i svůj subjektivní prognostický náhled na každou otázku, který bude na závěr dán do kontrastu se zjištěným stavem.

Poslední třetí část, tedy kapitoly 6 až 8, budou věnovány judikатурní oblasti GDPR, s důrazem v šesté kapitole na objasnění úřadu, který na problematiku s osobními údaji dohlíží. Tím je v České republice Úřad pro ochranu osobních údajů, kde bude čtenáři představena jeho role, obsazení a konečně bude poukázáno na jednotlivé reálné případy, jimiž se úřad v poslední době zabýval. Judikáty v kapitole 7 budou vybírány tak, aby byly pojmy popsané v předchozích kapitolách implementovány do soudních řízení, které probíhaly jak na tuzemském, tak evropském území. Předposlední kapitola nabídne čtenáři pohled do ochrany osobních údajů v zajímavých zahraničních aspektech.

Jak jsem již zmínil v úvodní části, cílem diplomové práce bude nabídnout čtenáři co nejkomplexnější přehled problematiky GDPR v pracovním právu, od čehož se odvíjí i koncept práce, který má čtenáře provést od vymezení základních pojmů a zásad, přes praktické obvyklé situace, se kterými je možné se běžně setkat na pracovišti, až po jednotlivé judikáty, které rozebírají GDPR v soudních řízeních.

2 Právní regulace GDPR

2.1 Historie právní úpravy osobních údajů

Historický kontext má nejen ve sféře práva velký vliv na momentální stav, ať je to v souvislosti s dlouhodobým, přirozeným a automatickým vývojem, nebo s nutností reakce na momentální událost. Právě tomuto se bude věnovat první podkapitola

Za celosvětově první právní předpis, který se nějakým způsobem dotýkal ochrany lidských práv, a tak vlastně i osobních údajů, neboť osobní údaj je lidské právo, je označována Deklarace práv člověka a občana (1789). Tento dokument přispěl pro vznik dalším právním dílům, týkajících se demokracie, a je tak brán jako odrazový můstek pro formování právního státu jako takového.

Nástup totalitních režimů a odkazu 2. Světové války zavedl vznik Všeobecné deklaraci lidských práv a svobod (1948). Z pohledu ochrany soukromí, a tedy i osobních údajů, je důležitý zejména článek 12 „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“¹. Z pohledu pracovního práva pak článek 23 odstavec 1 „Každý má právo na práci, na svobodnou volbu zaměstnání, na spravedlivé a uspokojivé pracovní podmínky a na ochranu proti nezaměstnanosti.“² S ohledem na postup práva jako takového tvoří zmíněný článek 23 zejména průlom v respektování důstojnosti na pracovišti ve smyslu nenarušování soukromí zaměstnance zaměstnavatelem a zasahováním do jeho osobnosti prostřednictvím zpracování osobních údajů.³

Všeobecná deklarace ale nikdy nebyla právní závaznost, stala se jakýmsi vyžadovaným standardem, nebo vyjádřením hodnot, které mají být

¹ Všeobecná deklarace lidských práv schválená Organizací spojených národů dne 10.12.1948

² tamtéž

³ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, 58 str.

dodržovány a respektovány. Právní závaznosti nabyl až Mezinárodní pakt o občanských a politických právech⁴, který v sobě⁵ přímo zakotvil výše citované z Deklarace.

Za zmínku stojí směrnice OECD z roku 1980. V této směrnici se poprvé objevují termíny jako „osobní údaj“ nebo „správce osobních údajů“, některé vůdčí principy a ideje této směrnice převzalo dokonce i Nařízení, vyskytují se zde práva jedinců, kterým jsou osobní údaje zpracovávány, jako je právo na informace o zpracování a právo podávat námitky proti zpracování. Vzhledem k tomu, že členskými státy OECD je také velké množství států mimo území Evropy, měla tato směrnice celosvětový dopad. Směrnice však není právně závazná a původně měla sloužit zejména jako návod pro vytvoření legislativy na ochranu osobních údajů v zemích, které doposud žádnou takovou právní úpravu neměly.⁶

Prvním právním dokumentem, který se zabýval čistě ochranou osobních údajů a standardizoval tak myšlenky z vyhlášky OECD, je možno označit Úmluvu č. 108⁷ a její dodatkový protokol⁸. Tuto Úmluvu podepsalo celkem 50 států, některé i mimoevropské, jako například Uruguay, či Senegal. Česká republika se k Úmluvě 108 připojila až o 20 let později, tedy v roce 2001. Úmluva 108 kodifikovala zásady, vycházející z předchozích právních předpisů, jako např.:

- a) *princip omezení sběru osobních údajů (správnost a legálnost);*
- b) *princip kvality osobních údajů (adekvátnost účelu, přesnost, úplnost a aktuálnost);*
- c) *princip specifikace účelu sběru osobních údajů (stanovení účelu musí předcházet začátku sběru dat);*

⁴ Mezinárodní pakt o občanských a politických právech a Mezinárodní pakt o hospodářských, sociálních a kulturních právech, publikované jako vyhláška ministra zahraničních věcí č. 120/1976 Sb.

⁵ Čl. 17

⁶ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. **GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář**. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 72

⁷ Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28.1.1981, publikovaná jako Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb.m.s.

⁸ Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice ze dne 8.11.2001, publikovaný jako Sdělení Ministerstva zahraničních věcí č. 29/2005 Sb.m.s

- d) *princip omezení užití osobních údajů (mohou být zpřístupněna nebo užitá jinak pouze se souhlasem subjektu údajů nebo na základě zákona);*
- e) *princip záruk bezpečnosti osobních údajů (musí být chráněna před ztrátou či neoprávněným přístupem, zničením, užitím, změnou nebo zveřejněním);*
- f) *princip otevřenosti (veřejnost informací o povaze a účelu zpracovávaných osobních dat a o jejich správci);*
- g) *princip účasti subjektu osobních údajů (právo na informaci o datech o něm sbíraných, právo na zpřístupnění jeho dat, právo na výmaz, opravu a doplnění);*
- h) *princip odpovědnosti správce osobních údajů (odpovídá za dodržování všech výše uvedených principů).⁹*

Následně byla v roce 1995 vydána Evropským parlamentem směrnice 95/46/ES¹⁰. Směrnice byla tvořena 72 recitály a 34 články, které komplexně a jednotně upravila pro členské státy právní úpravu pro zajištění fungování jednotného trhu a účinnou ochranu základních práv a svobod. Směrnice 95/46/ES byla implementována do českého právního řádu pomocí zákona o ochraně osobních údajů¹¹, který byl několikrát novelizován.¹² Směrnice a tedy i zákon o ochraně osobních údajů¹³ přestaly být účinnými v České republice 25. Května 2018 nástupem GDPR.

GDPR a česká legislativa

Nařízení tedy nahradilo zákon o ochraně osobních údajů a stanovilo nová pravidla pro zpracování osobních údajů. GDPR se vztahuje na subjekty, které spravují nebo zpracovávají osobní údaje, včetně státních orgánů jako jsou Úřad pro ochranu osobních údajů, soudů a inspektorátů práce. Avšak na činnosti, při kterých jsou zpracovávány osobní údaje výlučně pro osobní účely se GDPR nevztahuje. Stejně tak se GDPR nevztahuje na zpracování osobních údajů

⁹ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, str. 67

¹⁰ Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

¹¹ Zákon č. 101/2000 Sb., zákon o ochraně osobních údajů

¹² NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 72

¹³ Zákon č. 101/2000 Sb., zákon o ochraně osobních údajů

prováděné příslušnými orgány za účelem prevence, vyšetřování a stíhání trestných činů, což je upraveno samostatnou směrnicí Evropského parlamentu a Rady 2016/680 ze dne 27. dubna 2016. Jelikož se jedná o směrnici a nikoli o nařízení, není zde povinnost přímé implementace členským státem do svého právního řádu, proto jisté stopy této směrnice je možné zpozorovat například v zákonu o Policii ČR¹⁴, v zákonu o zpracování osobních údajů, popřípadě v jiných právních předpisech.

2.2 Předmět a cíle

Druhá podkapitola bude komplexně popisovat předmět a cíle Nařízení, jednoduše řečeno, popíše důvod a účel samotného předpisu.

Předmět a cíle GDPR jsou uvedeny v článku 1 Nařízení. Předmětem GDPR jsou pravidla týkající se práv fyzických osob v souvislosti s osobními údaji a jejich pohybem. Osoby chrání GDPR jednak tak, že jim přiznává určitá práva, se kterými mohou disponovat v rámci kontroly nad využíváním jejich osobních údajů, a také reguluje podmínky pro ty, které jejich osobní údaje zpracovávají.¹⁵

Cíle GDPR jsou uvedené v témže článku ve druhém odstavci. Především se jedná o ochranu osobních údajů v souvislosti s rostoucím vlivem moderních technologií, jako jsou sociální sítě, internet i s ohledem na elektronické bankovníctví a obchodování. V návaznosti právě na rozvoj těchto aspektů, byla směrnice 95/46/ES již zastaralá a její inovaci bylo možné řešit pouze novelami. Další důvod vzniku GDPR byla samotná povaha právního předpisu. Jelikož původní směrnice 95/46/ES nezavdávala členským státům povinnost přímé implementace do jejich právních řádů, vydala EU právě nařízení, které zavazuje členské státy k implementaci a k unifikačnímu efektu, který má za cíl vytvořit jednotnost pravidel pro celou EU.¹⁶

2.3 Věcná působnost

V první řadě je nutné si vymežit definici věcné působnosti GDPR což

¹⁴ Zákon č. 273/2008 Sb., Zákon o Policii ČR.

¹⁵ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVÁŘIKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 75

¹⁶ NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, str. 31

uvádí Žůrek jako „vztahy, které právní předpis upravuje, tedy na co se vztahuje (pozitivní vymezení), případně na co se nevztahuje (negativní vymezení). Obecné nařízení obsahuje jak pozitivní, tak negativní vymezení věcné působnosti.“¹⁷ V této souvislosti je proto potřeba uvést čl. 2 Nařízení, kde je uvedena právě pozitivní i negativní stránka věcné působnosti tohoto předpisu.

Mezi pozitivní, upravené v odst. 1 tohoto článku, tedy na ty, na které se Nařízení vztahuje, je řazeno zpracování osobních údajů, ať už zcela nebo částečně automatizované, a těch údajů, které obsahuje evidence a nebo do ní mají být časem zařazeny.¹⁸ Smysl této formulace je spatřován v tom, že ač Nařízení počítá s převahou celkové automatizace, neopomíná právě možnost obsažení osobních údajů v evidenci, tedy ve formě jakékoliv jiné, než právě té automatizované.

Negativní věcnou působnost, tedy taxativně vyjmenované případy, na které se Nařízení nevztahuje, upravuje odstavce 2 článku 1. Lze tedy konstatovat, že GDPR dopadá na všechny ostatní případy, které v tomto odstavci nebudou uvedeny. Je to v první řadě takové zpracování osobních údajů, které osoba používá výhradně k domácí nebo osobní činnosti. Jako příklad je možné uvést např. vedení vlastních záznamů, korespondenci, vytváření adresářů nebo využívání sociálních sítí bez jakékoliv souvislosti s obchodní nebo profesní činností.¹⁹ V této souvislosti je ale nutné uvést judikát SDEU C-101/01 Lidquist, „*kdy soudní dvůr judikoval, že i samotné zveřejnění informací o jiné fyzické osobě na webové stránce je zpracováním osobních údajů, které navíc nespadá do výjimky pro osobní a domácí činnosti. Za zpracování osobních údajů je proto nutné v souladu s výše uvedeným považovat jejich zveřejnění na osobních blozích či otevřených profilech na sociálních sítích, které do působnosti výjimky nespadnou.*“²⁰ Stejný případ se týká také sledování kamerou, byť jen částečně, veřejného prostranství. Dalším případem vyňatým z věcné příslušnosti jsou

¹⁷ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 34

¹⁸ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 78

¹⁹ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 35

²⁰ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 79

osobní údaje zesnulých osob, jehož problematiku upravuje vnitrostátní právní řád.²¹

2.4 Místní působnost

Stejně jako u věcné působnosti bude nejprve definován pojem místní působnost, který podle Žúrka znamená „*omezení právního předpisu na určité území, zejména na to, kde lze jeho aplikaci efektivně vymáhat prostřednictvím dozorových úřadů.*“ Právní úprava místní působnosti kotví v článku 3, odstavce 1 až 3 Nařízení. Jelikož se jedná o nařízení EU, je proto dané, že z geografického hlediska, tedy teritoriálního území, se bude týkat členských států EU. Nařízení ale dopadá z důvodu možné snahy správců a zpracovatelů obejít právní následky i na takové zpracování osobních údajů, které se týká činnosti provozovny v EU, nehledě na to, zda reálně probíhá v či vně EU. Poté je nutné si objasnit pojem provozovna, který znamená reálnou aktivitu nebo činnost, u které není relevantním aspektem právní forma.²²

Extrateritoriální působnost

Odstavec 2 článku 3 Nařízení se zabývá tzv. extrateritoriální působností Nařízení, kde za účelem ochrany osobních údajů uvádí dva případy, které se vztahují i na správce a zpracovatele, kteří nemají sídlo na území EU a neprovozují zde činnost prostřednictvím provozovny, kterou je popsána výše. Týká se to správců a zpracovatelů, kteří

- a) *nabízejí zboží nebo služby subjektům údajů v EU*, (jako příklad si u tohoto bodu můžeme uvést klasický e-shop z Asie, který zde nemá provozovnu, ale prostřednictvím internetu zde nabízí nějaký produkt, a subjekt osobních údajů, nacházející se v EU, mu své údaje poskytne.)
- b) *nebo monitorují jejich chování, pokud k němu dochází v EU*²³. (zde bych jako příklad uvedl tzv. cookies v souvislosti s používáním internetových stránek.)

Jako základní předpoklad pro vznik extrateritoriální místní působnosti je

²¹ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 36

²² tamtéž

²³ Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 3(2)

možné nazvat zpracování, uchovávání a nakládání s osobními údaji subjektu, jenž se nachází v EU. Z Extraterritoriality ale nevyplývá to, že pokud by fyzická osoba vycestovala do země, která není členským státem EU, bylo by jí zavdáno stejné ochrany osobních údajů, jako by tomu bylo na území EU. Proto je potřeba rozeznat a uvědomit si, že samotná ochrana nařízení podle jeho místní působnosti necílí na občana EU jako takového a přiznávala by mu práva, která uvádí, ale výhradně na místo výskytu subjektu údajů.²⁴

²⁴ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 37

3 Základní pojmy a principy

V třetí kapitole diplomové práce přejdu k jednotlivým pojmům a principům, které tvoří samotné Nařízení, a na jejichž bázi je tvořen. V osmi podkapitolách budou popisovány nejpodstatnější a nejvíce frekventované pojmy a zásady, které se objevují jak v Nařízení, tak v diplomové práci, a pochopení jejich smyslu je tak nutné pro pochopení celého GDPR.

3.1 Osobní údaj

Osobní údaj představuje nejvýznamnější pojem, jelikož právě kvůli němu, jeho ochraně a používání, vzniklo GDPR. Jeho definice se ve srovnání se směrnicí 95/46ES nezměnila. Formulaci uvádí článek 4 odstavec 1 Nařízení, kde jsou taxativně zmíněny aspekty osobního údaje a zní „*Pro účely tohoto nařízení se rozumí: „osobními údaji“ veškeré informace o identifikované fyzické osobě (subjektu údajů); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo nebo nepřímo identifikovat, zejména odkazem na určitý identifikátor, nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické kulturní nebo společenské identity této osoby.*“²⁵ Větší důraz, vzhledem k většímu vlivu internetu, klade Nařízení na rozšíření identifikátorů, které lze brát jako osobní údaj, jako je například IP adresa, nebo soubory cookies. Subjektem údajů je tak fyzická osoba, dotčená osobními údaji, na rozdíl třeba od údajů, které se týkají právnických osob.

Za osobní údaj lze tedy označit jakoukoliv informaci, která jakýmkoliv způsobem vede k identifikaci fyzické osoby, zde je tradičně uváděno jako příklad jméno, příjmení, adresa trvalého pobytu, emailová adresa, atd. Nebo i informaci, která zasahuje do její osobnostní sféry, zde bych z pohledu pracovního pracovního práva uvedl údaje o platu nebo označením pracovní pozice, která je zastávána.²⁶

Citlivé osobní údaje

Jisté specifikum mají citlivé osobní údaje, kterým, ve smyslu nakládání

²⁵ Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 1 (2)

²⁶ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, str. 128

s nimi, jsou dány přísnější podmínky, neboť jejich povaha více zasahuje do integrity osoby. Jejich výčet je uveden ve článku 9, odstavec 1 Nařízení a jsou jimi osobní údaje, které vedou k identifikaci osoby na základě jeho „*rasového či etnického původu, politických názorů, náboženského vyznání či filozofického přesvědčení nebo členství v odborech, o zdravotním stavu, sexuální životě a sexuální orientaci fyzické osoby. Za zvláštní kategorii osobních údajů se považují i genetické a biometrické údaje, avšak pouze pokud jsou zpracované za účelem jedinečné identifikace fyzické osoby*“²⁷ Z tohoto výčtu definuje Nařízení v článku 4 dále pouze genetické údaje, biometrické údaje a údaje o zdravotním stavu.²⁸ Při zpracování citlivých údajů je nutný výslovný souhlas subjektu.

3.2 Správce, zpracovatel

Druhá podkapitola, pojednávající o dalších klíčových pojmech, je správce a zpracovatel. Úprava GDPR se příliš neodchýlila od původní směrnice 95/46/ES, definuje jej ve článku 4 odstavec 7 Nařízení. Správce, který může být jak fyzická, tak právnická osoba, lze označit jako hlavního adresáta povinností, kterého Nařízení zavazuje, ale zároveň určuje prostředky a účel zpracování.

Nařízení stanovuje, že každý, kdo zpracovává osobní údaje, se stává správcem osobních údajů a nese odpovědnost za ochranu těchto údajů. To znamená, že správce musí dodržovat určité povinnosti, jako je například respektování práva subjektů údajů na ochranu svého soukromí a na informovanost o zpracování svých údajů.²⁹

Nařízení dále rozlišuje dva typy situací, kdy se osoba nebo subjekt stává správcem osobních údajů. První situace je, když se osoba rozhodne zpracovávat osobní údaje z vlastní iniciativy, například při instalaci kamerového systému v bytovém domě. V této situaci musí správce určit všechny parametry zpracování osobních údajů v souladu s Nařízením. Druhá situace je, když se osoba stane správcem osobních údajů v důsledku své činnosti v návaznosti na zákonné povinnosti. To znamená, že zpracování osobních údajů je nutné pro splnění těchto povinností, jako je například uzavření pracovněprávního vztahu nebo

²⁷ Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 9 (1)

²⁸ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 52

²⁹ MORÁVEK, J. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019, str. 164

výpočet sociálního a zdravotního pojištění. V této situaci je účel zpracování osobních údajů stanoven právními předpisy, podle kterých se správce řídí. V obou situacích musí správce dodržovat například určení účelu zpracování, rozsahu zpracovávaných osobních údajů, doby uchování údajů a zajištění bezpečnosti osobních údajů. Dále platí pro správce povinnost subjekt informovat o zpracování osobních údajů subjektu a jejich právo na výmaz nebo přístup.³⁰

Účelem se rozumí cíl konkrétní činnosti a jeho smysl, prostředky pak alternativy pro zpracování.³¹ Další možností správcovství je zřízení dvou nebo více správců, pro které je typické, že je zmíněné účely a prostředky určí mezi sebou. Zpracování údajů v některých případech není závislé pouze na správci a to v situaci, když správce pověří zpracovatele, jehož úlohu definuje článek 4 odstavec 8. Dle Nařízení je ale jediný možný subjekt oprávněný o rozhodování ve věci zpracování správce, proto zpracovatel pouze vykonává činnost přidělenou správcem a nemůže se od ní odchýlit. K najmenování zpracovatele dochází nejvíce z důvodu absencí technických nebo personálních prostředků ze strany správce, což se naopak očekává od zpracovatele, tedy odborná i technologická zdatnost. Je podstatné ale zmínit, že samotná odpovědnost správce nikdy nezmizí a nepřechází určením zpracovatele čistě na něj. Jejich vzájemná práva a povinnosti nejčastěji upravuje „smlouva o zpracování osobních údajů“ a to v případech, když nevzniká tzv. „zákonné zmocnění“.³² Správce také může najmenovat více zpracovatelů a zpracovatel další zpracovatele, pak by se hovořilo o řetězení zpracovatelů.

3.3 Pověřenec pro ochranu osobních údajů

Celkem specifická a nová funkce díky GDPR z pohledu nutnosti existence je pověřenec pro ochranu osobních údajů, který je zřízen správcem nebo zpracovatelem. Nařízení mu předpisuje minimální výčet úkolů, uvedených ve článku 39 Nařízení, které musí vykonávat, jejich počet však není zastropován. Jsou to:

³⁰ tamtéž

³¹ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 95

³² ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 85

- a) *Poskytování informací a poradenství správcům a zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany údajů.*
- b) *Monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů*
- c) *Poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle článku 35 Nařízení*
- d) *Spolupráce s dozorovým úřadem*
- e) *Působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci³³*

Jeho úloha spočívá v kooperaci se správcem, být mu nápomocný ve snaze chránit práva a povinnosti subjektů údajů.³⁴ Dále má shromažďovat informace za účelem zjišťování zpracovatelských činností a analyzovat a prověřovat právní soulad zpracovatelských činností.³⁵ Pověřenec má fungovat na bázi nezávislého postavení vůči správcově organizaci a dle Nařízení a jeho povinností mu nesmějí být ukládány žádné konkrétní úlohy. Tato funkce není obligatorní, správce nemusí pověřence zřizovat ani zdaleka vždy, v současnosti má ale čím dál více správců k dispozici zaměstnance nebo skupinu zaměstnanců, kteří se starají právě o osobní údaje specificky a konkrétně.³⁶

³³ Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 39

³⁴ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 105

³⁵ NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, str. 277

³⁶ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 296

Je možné ale pověřence rozdělit do dvou skupin a to do interních, kdy správce určí pověřence z řad uvnitř společnosti, kde lze označit za výhodu znalost prostředí a lepší koncept komunikace, za nevýhodu potencionální riziko střetu zájmů a specifickou úpravu ukončení pracovního poměru. Druhou skupinou jsou pověřenci externí, tedy že nemají žádný zaměstnanecký vztah ke správci. Jejich výhodami je neutrální postavení ke správci, tedy že nevzniká střet zájmů a odbornější způsobilost. Za nevýhody lze považovat neznalost konkrétního prostředí ve společnosti a nedostatek interních kapacit.³⁷ Jsou ale konkrétní taxativně vyjmenované situace ve článku 37 odstavec 1, kdy pověřenec být jmenován musí, konkrétně jsou to:

- a) *Zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí (tedy subjekty založené veřejnoprávním předpisem)*
- b) *Hlavní činností spočívající v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektu údajů*
- c) *Hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v čl. 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10³⁸*

Pověřenec jako takový nemusí být nutně erudovaným odborníkem na IT, právní oblast, nebo bezpečnost, stačí pouze, aby vykonával jemu zadané úkoly podle článku 39 Nařízení, měl hlubokou znalost Nařízení a dokázal se pohybovat ve vnitrostátních a mezinárodních předpisech. Nadále by měl splňovat požadavky určité morální a etické vyspělosti, která by mu pomohla v konstruování kulturní stránky ochrany osobních údajů. Úroveň pověřencovy způsobilosti by měla odpovídat komplikovanosti a citlivosti konkrétních údajů, tedy, že složitější formulace bude vyžadovat vyšší kvality pověřence.³⁹

³⁷ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 300

³⁸ Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 37 (1)

³⁹ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J.,

3.4 Zpracování osobních údajů

Při představení pojmu zpracování osobních údajů je důležité zmínit, že zpracování nepředstavuje každou činnost, kdy je nakládáno s osobními údaji, jelikož by se pak jednalo o každé lidské jednání, které by obsahovalo jakékoliv údaje subjektu. Tímto pojmem se rozumí soustavné a operativní jednání správce osobních údajů, které systematicky, ať už automatizovaně nebo jinými prostředky, vykonává.⁴⁰ Z pohledu správce se tak bude zejména jednat o shromažďování, ukládání, zpracovávání a přenášení informací, které se týkají určitého jedince v rámci pracovního vztahu, které budou využívány pro předem dané legitimní účely, které jsou uvedeny v článku 6 Nařízení, a musí být splněna alespoň jedna z podmínek v tomto článku uvedených.

Právo na výmaz

Správce osobních údajů má podle Nařízení povinnost vymazat osobní údaje na žádost subjektu údajů pouze tehdy, jsou-li naplněny podmínky uvedené v článku 17 odstavec 1 Nařízení a zároveň nelze použít žádnou z výjimek uvedených v odstavci 3 téhož článku. Avšak obvykle má správce povinnost vymazat osobní údaje sám, tedy bez žádosti subjektu údajů, pokud účel zpracování již neexistuje, protože to vyžaduje zásada omezení uložení osobních údajů podle článku 5 Nařízení.

V každém případě musí správce osobní údaje vymazat, pokud subjekt údajů požádá a splňuje se alespoň jedna z následujících podmínek:

- a) *Správce nepotřebuje osobní údaje pro účely, pro které byly shromážděny*
- b) *Subjekt údajů odvolá svůj souhlas se zpracováním osobních údajů*
- c) *Subjekt podá námitku proti zpracování svých údajů a správce nemá*

KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 298

⁴⁰ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 54

oprávněný zájem na zpracování těchto údajů

- d) *Osobní údaje byly shromážděny protiprávně*
- e) *Na správce se vztahuje právní povinnost vyplývající z práva EU nebo z práva členského státu, která mu ukládá osobní údaje vymazat.*⁴¹

3.5 Omezení zpracování osobních údajů

Subjekt údajů má dle Nařízení ale právo na omezení zpracování jeho osobních údajů. To znamená, že správce musí omezit zpracování za předpokladu naplnění podmínek uvedených ve článku 18 odstavec 1 Nařízení, tedy:

- a) *subjekt údajů popírá přesnost osobních údajů – omezení se vztahuje na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit,*
- b) *zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití,*
- c) *správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků,*
- d) *subjekt údajů vznesl námitku proti zpracování – omezení se vztahuje na dobu dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů. Pokud bylo zpracování omezeno, mohou být tyto osobní údaje, (s výjimkou jejich uložení), zpracovány pouze:*
 - 1. *se souhlasem subjektu údajů,*
 - 2. *z důvodu určení, výkonu nebo obhajoby právních nároků,*
 - 3. *z důvodu ochrany práv jiné fyzické nebo právnické osoby*
 - 4. *z důvodů důležitého veřejného zájmu Unie nebo některého členského státu.*⁴²

Jinak řečeno, subjekt, o kterém se jedná v osobních údajích, má právo požadovat od správce, aby omezil zpracování svých údajů ve výše uvedených případech. Ve shrnutí se tak tato práva vztahují na případy, kdy subjekt požaduje opravu svých osobních údajů, kdy správce zpracovával jeho údaje v rozporu se zákonem, kdy už správce údaje nepotřebuje pro účely

⁴¹ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 196

⁴² Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 18

zpracování, ale subjekt údajů je potřebuje pro právní účely, a kdy subjekt údajů vznesl námitku proti zpracování. Omezení zpracování údajů má za účel zabránit jejich neoprávněnému zpracování a porušení zákona, a to zejména v případech, kdy by vymazání údajů porušilo práva subjektů.⁴³

3.6 Zásada zákonnosti, korektnosti a transparentnosti

Zpracování údajů i celé Nařízení má svůj základ ve vůdčích idejích, podle kterých se řídí. Následující podkapitola se bude zabývat zásadami, které jsou stěžejní pro koncept celého GDPR.

Zásada zákonnosti

Zásada zákonnosti, jako ve všech odvětvích práva, je ta nejvíce relevantní, neboť zavazuje správce k právnímu důvodu zpracování. Pokud tento důvod pomine, je správce povinen osobní údaje zlikvidovat. Každý správce osobních údajů musí naplňovat alespoň jeden z právních důvodů uvedených ve článku 6 odstavec 1 Nařízení a pro kategorii zvláštních osobních údajů ve článku 9 odstavec 2 Nařízení.⁴⁴ Tato zásada též stanovuje, že nakládání s údaji nesmí být pouze v rozporu s Nařízením, ale také s právním řádem jako celkem, což značí, že pokud bude konkrétní situace v souladu s Nařízením, ale půjde *contra legem* vnitrostátního předpisu, bude nepřipustné.

Zásada korektnosti a transparentnosti

Zásada korektnosti a transparentnosti má své podstaty v tom, že správce nemůže zastírat důvod zpracovávání osobních údajů. Konkrétně zásada transparentnosti zavazuje správce informovat subjekt o rozsahu zpracování jeho údajů s ohledem na článek 13 a 14 Nařízení.⁴⁵ S touto zásadou je možné se setkat v případě porušení zabezpečení ochrany osobních údajů, je-li správce povinen oznámit tuto skutečnost dozorovému úřadu, tak i subjektu údajů.⁴⁶ Podle zásady korektnosti musí správce údajů se subjektem jednat na základě pravdy a

⁴³ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 202

⁴⁴ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 58

⁴⁵ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 110

⁴⁶ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 60

skutečnosti. K porušení této zásady dochází nejčastěji z důvodu nedostatečného informování ze strany správce nebo pokud bude uváděn v omyl.⁴⁷

3.7 Zásada minimalizace údajů

Tato zásada spočívá v povinnosti správce uchovávat osobní údaje subjektu pouze v takové rovině, která je nezbytná pro daný účel. Musí tedy dodržovat míru přiměřenosti a nezbytnosti s nakládáním těchto údajů. Je zde i spatřován jistý bezpečnostní prvek proti nechtěnému úniku.⁴⁸ V této souvislosti se nabízí test proporcionality, který určí požadované nezbytné množství zpracovávaných osobních údajů.

Ve sféře pracovního práva se touto problematikou zabývá §30, §312 a §316 Zákoníku práce⁴⁹⁵⁰, který zaměstnavateli určuje, že může před vznikem pracovního poměru požadovat po zaměstnanci pouze ty údaje, které souvisí s jeho potencionálním uzavřením pracovní smlouvy.

3.8 Zásada přesnosti

Dle této zásady mají být údaje subjektu přesné a odpovídat skutečnosti. V praxi se tato zásada uplatní například v situaci, když dojde k písařské chybě u některých údajů (jméno, email). Správce je tak oprávněn bez souhlasu subjektu tento údaj opravit. Je tak předcházeno problémům, když je subjekt kupříkladu limitován absencí důležitých informací rozesílaných do služebního emailu.

4 GDPR v jednotlivých fázích pracovního poměru

V dalších kapitolách přejdu od oblastí vzniku, struktury a principů k jádru diplomové práce a to vlivu GDPR na pracovní právo. Postupně popíšu jeho dopad chronologicky v jednotlivých fázích pracovního poměru, tedy před, během

⁴⁷ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 110

⁴⁸ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 61

⁴⁹ Zákon 262/2006 Sb., Zákoník práce

⁵⁰ MORÁVEK, J. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, 2019, str. 215

a po ukončení.

4.1 Zpracování osobních údajů před uzavřením pracovního poměru

První podkapitola bude lehce atypická už z aspektu jejího názvu. Nabízí se zde otázka, zda potenciální správce, tedy zaměstnavatel, může vůbec zpracovávat osobní údaje subjektu, se kterým nemá uzavřený žádný právní vztah, v tomto případě pracovní poměr. Zaměstnavatel logicky musí operovat s osobními údaji subjektu před vznikem jeho pracovního poměru a stává se tak jejich správcem. Tyto osobní údaje ale musí být v souladu se zásadou proporcionality a minimalizace, tedy, že může být vyžadováno pouze toliko údajů, které bezprostředně souvisí s výkonem jeho budoucího povolání. Jako zákonný základ lze uvést §30 zákoníku práce.

V praxi tak je možné uvést příklad, když zaměstnavatel podá inzerát na volné pracovní místo a potenciální uchazeč zašle svůj životopis, který obsahuje nemálo osobních údajů. Zaměstnavatel tedy v tento okamžik již zpracovává osobní údaje, v tomto případě životopis, uchazečů. V situaci, kdy uchazeč nebude vybrán, tedy s ním nebude uzavřena pracovní smlouva, tak mu musí zaměstnavatel zasláný životopis vrátit nebo jej zlikvidovat. Jestliže mu ale uchazeč udělí souhlas se zachováním jeho životopisu, například pro okamžiku vzniku nové pracovní pozice, musí zaměstnavatel zřídit jakousi databázi potenciálních uchazečů, kde bude jeho životopis uchován. V praxi je snadno představitelné například zařazení do databáze filmové castingové agentury, kdy uchazeč nebyl vybrán pro konkrétní snímek, ale může být vybrán na další.⁵¹

Podání inzerátu a zaslání životopisu ale není jedinou možnou alternativou, kdy je možné se setkat se zpracováním osobních údajů ještě před uzavřením pracovního poměru. Velmi často se využívají různé internetové portály, nebo přímo sociální sítě, kdy si uchazeč vytvoří svůj profil a čeká, jestli mu nějaká nabídka pracovního místa nepřijde ze strany zaměstnavatele (v tomto případě bych uvedl velmi populární síť LinkedIn). Úlohu správce osobních údajů zastává konkrétní portál, kde subjekt údajů udělil souhlas se zpracováním podle článku 6 odstavce 1 Nařízení.

⁵¹ BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5.

Diskriminace před uzavřením pracovního poměru

Důležitý aspekt je v souvislosti s výběrem zaměstnanců do pracovního poměru zákaz diskriminace, neboť některé osobní údaje k ní mohou vést, v souvislosti s antidiskriminačním zákonem. Znaky diskriminace může naplňovat už sám podaný inzerát. Zakázaná je diskriminace jak pozitivní, tak negativní. Nejčastější je zřejmě diskriminace z důvodu pohlaví, vyskytují se ale další důvody, jako je věk, národnosti, fyzické parametry (výška, váha). Zaměstnavatel tedy nemůže inzerovat cíleně mířený požadavek na pohlaví, je-li pracovní pozice reálně vykonatelná mužem i ženou – přípustný by byl inzerát „přijmeme pracovní sílu do kuchyně“. Nepřípustný by byl „přijmeme kuchařku do kuchyně.“ Pokud se ale jedná o případ, že by bylo narušeno BOZP⁵², například při pracovní pozici horníka, nebo skladníka při manipulaci s těžkými břemeny, může zaměstnavatel mířit přímo na konkrétní pohlaví. Těžko je také představitelné, že by muž hrál postavu Rusalky, neboť by mu to jeho hlasové a fyzické předpoklady neumožnily, proto je v tomto případě také nediskriminační, pokud Státní opera bude mířit přímo na ženské pohlaví.

4.2 Zpracování osobních údajů za trvání pracovního poměru

Druhá podkapitola bude věnována jádru zpracování osobních údajů v souvislosti s pracovním poměrem. Jedná se o nejužší a nejintenzivnější vztah mezi zaměstnavatelem a zaměstnancem ze všech fází. Pracovní poměr vzniká uzavřením pracovní smlouvy a její účinností začínají platit nová práva a povinnosti. To se nepochybně dotýká i osobních údajů, neboť před začátkem pracovního poměru, jak je popsáno v podkapitole 4.1, byl zaměstnavatel více právně limitován, než tomu je při trvání. V tomto případě lze odkázat na článek 6 odstavec 1 písmeno c) Nařízení. Už při podpisu pracovní smlouvy je možné se setkat s tím, že v některých smlouvách správce uvede formulaci, že zaměstnanec souhlasí se zpracováním osobních údajů. Takový souhlas je ale podle Žůrka neplatný, matoucí zaměstnance, který si myslí, že může souhlas v budoucnu odvolat. Žůrek dále uvádí, že „*má-li zaměstnavatel pracovní smlouvy s takovým souhlasem již uzavřeny, neznamená to jejich neplatnosti či nemožnost zpracovávat osobní údaje zaměstnance pro pracovněprávní účely, protože zaměstnavateli svědčí právní důvod plnění smlouvy a plnění zákonem stanovené*

⁵² Bezpečnost a ochrana zdraví při práci

*povinnosti, případně právní důvod nezbytnosti pro účely jeho oprávněných zájmů či třetí strany. Jelikož takový souhlas nebude využitelný, je vhodné jej do budoucna vypustit a místo něj poskytnout zaměstnanci informace ve smyslu článku 13 Nařízení.*⁵³

Osobní spis

Důležitý pojem při pracovním poměru s souvislostí se zpracováním osobních údajů je osobní spis zaměstnance. Zaměstnavatel může spis vést podle §312 zákoníku práce. Osobní spis je soubor dokumentů vedený zaměstnavatelem, který obsahuje informace o zaměstnanci, jako jsou identifikační údaje, záznamy o zaměstnancově vzdělání, pracovních zkušenostech, výkonnosti, absencích, platových údajích a dalších relevantních informací. Spis je veden za účelem řízení personálních záležitostí, jako je například hodnocení výkonu, plánování kariéry nebo poskytování zaměstnaneckých výhod, nicméně musí obsahovat pouze informace, které se týkají výkonu práce. Zaměstnanec má právo na přístup ke svému osobnímu spisu a může požadovat opravu nebo doplnění informací, které jsou v něm obsaženy. Odlišně je zacházeno s citlivými údaji, tedy s informacemi, které se týkají zaměstnance kvůli jeho „*rasovému či etnickému původu, politických názorech, náboženskému vyznání či filozofickému přesvědčení nebo členství v odborech, o zdravotním stavu, sexuálním životě a sexuální orientaci fyzické osoby. Za zvláštní kategorii osobních údajů se považují i genetické a biometrické údaje, avšak pouze pokud jsou zpracované za účelem jedinečné identifikace fyzické osoby*“⁵⁴ Takové informace může v osobním spise zaměstnavatel uchovávat pouze s výslovným souhlasem zaměstnance, který je zaměstnavatel povinen prokázat po celou dobu trvání pracovního poměru, nebo pokud mu to nedovoluje zvláštní zákon.⁵⁵

Nařízení ve svém článku 5 odstavec 1 písmeno f) zavazuje zaměstnavatele zajistit důvěrnost a integritu osobních údajů. Jelikož osobní spis obsahuje údaje subjektu, musí být předcházeno riziku úniku těchto údajů. Morávek rozděluje tři

⁵³ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 71

⁵⁴ Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 9 (1)

⁵⁵ BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5., str. 148

opatření na úseku bezpečnosti a jsou jimi:

- a) *Personální – Určení okruhu osob, které budou mít k osobním údajům přístup, dispozic, které s nimi mohou činit a případů, kdy k nim mohou přistoupit, přičemž zejména při větší specializaci činností u zaměstnavatele či více vedoucích zaměstnancích s přístupem do osobního spisu zaměstnance, nelze v návaznosti na šíři dokumentace a rozsah osobních údajů zařazených do osobního spisu vyloučit diferenciaci uživatelských oprávnění, tzn., že do určitých částí osobního spisu budou mít přístup jen zaměstnanci na určitých pracovních pozicích. Jako oprávněného pro nahlížení do spisu můžeme označit zaměstnavatele, vedoucího zaměstnance, nebo zaměstnance, který díky jeho pozici a účelu přístup do spisu vyžaduje.*
- b) *Prostorové – prostorová bezpečnost by, pokud možno, měla odrážet opatření vyplývající z personální bezpečnosti (např. klíče ke kartotéce by měli mít jen oprávnění zaměstnanci), současně by měly reflektovat obecné hrozby pro osobní údaje a jejich nosiče (riziko krádeže, zničení, pořízování kopií..)*
- c) *Výpočetní technika – bezpečnost IT by se měla odrážet z vyplývajících personální bezpečnosti (přístup by měly mít pouze oprávněné osoby a pouze ve stanovených případech), dále by bezpečnost výpočetní techniky měla obsahovat bezpečnostní prvky typu antivirového programu, šifrování, zálohování údajů, atd..⁵⁶*

Zaměstnavatel se vedením osobního spisu stává správcem dle článku 4 odstavce 7 Nařízení, který může využít zpracovatele článek 4 odstavec 8 Nařízení. Při této situaci se očekává ještě úprava vzájemných poměrů, tedy zejména určení a ochrana zpracovávání údajů. Při nechtěnému úniku, ztrátě nebo neoprávněnému přístupu podle článku 4 odstavce 12 Nařízení musí správce tuto skutečnost oznámit dozorovému úřadu i subjektu údajů.⁵⁷ Samotné poskytování osobních údajů, tedy seznámení se s informacemi z osobního spisu, může kromě

⁵⁶ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, str. 354

⁵⁷ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, str. 350

zaměstnavatelů, vedoucích zaměstnanců a určitých zaměstnanců Úřad práce České republiky, ÚOOÚ, soud, státní zástupce, policejní orgán, Národní bezpečnostní úřad a zpravodajské služby.⁵⁸ Všechny osoby, které do spisu nahlízejí a mají přístup, jsou vázány mlčenlivostí.

Osobní spis ale není jediným instrumentem zpracování osobních údajů zaměstnavatelem. Jako příklad lze uvést § 105 zákoníku práce, podle kterého eviduje v knize úrazů záznamy o všech úrazech zaměstnanců, kvůli kterým byli v pracovní neschopnosti nepřesahující 3 kalendářní dny. Má také ale povinnost zranění zaměstnanců s pracovní neschopností přesahující 3 kalendářní dny, nebo úmrtí. Dále má povinnost dokumentovat zaměstnance, u kterých byla diagnostikována nemoc z povolání.⁵⁹ U této skutečnosti nastává otázka, zda citlivý údaj uvedený v článku 4 odstavec 15 Nařízení, což informace o zdravotním stavu zaměstnance nepochybně jsou, může být zaměstnavatelem evidován. Je nutné si uvědomit, že s odkazem na §103 odstavec 1 písmeno c) zákoníku práce, je zaměstnavatel povinen zaměstnávat osoby, které mají zdravotní způsobilost vykonávat určitou činnost, kde je tomu vyžadováno. V praxi by se jednalo o osvědčení vykonávat pracovní pozici vyžadující zdravotní průkaz, nebo nutnosti očkování, respektive osvědčení o odolnosti vůči nemoci. Zaměstnavatel také zpracovává údaje o svých těhotných zaměstnankyních, což je informace, která se přímo zdravotního stavu netýká, ale jistá citlivost zde upozorovat jde. Zaměstnavatel tuto informaci zpracovává hlavně proto, aby předcházel rizikům, respektive, aby se dbalo zvýšené opatrnosti při výkonu práce těhotných zaměstnankyň a je také povinen tyto zaměstnankyně informovat o zdravotních rizicích, to ale neplatí v případech, když zaměstnankyně o svém těhotenství zaměstnavatele neinformuje. V Nařízení se touto problematikou zabývá Recitál 53, který specifikuje tyto údaje jako jedinečné číslo nebo symbol přidělené subjektu, podle kterého by se konkrétně identifikovaly zdravotní potřeby zaměstnance.⁶⁰

⁵⁸ BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5., str. 159

⁵⁹ BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5., str. 161

⁶⁰ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 54

Zajímavý aspekt při zpracovávání osobních údajů přichází v úvahu v okamžiku docházkového systému založeném na bázi zobrazení obličeje, nebo daktyloskopických údajů, což lze dle článku 4 odstavce 14 Nařízení považovat za biometrický údaj. Praxe výkladu ÚOOÚ je taková, že pokud se neukládá přímo otisk prstu nebo kontura obličeje, ale systém pracuje na základě haše, což je algoritmus náhodných písmen a čísel, tedy, že je nadále pracováno pouze s touto sekvencí, nejedná se o zpracování citlivého údaje. Tomu by tak bylo, pokud by se operovalo přímo s biometrickým údajem.

V otázce údajů o mzdě nebo platu zaměstnance, které bývají velmi osobní, má přístupovat správce údajů tak, že v žádném případě nemají být transparentní, přístup k nim má mít jen vymezený okruh osob a mají být zpracovávány v souladu s právními předpisy.⁶¹

Za další evidenci osobních údajů je možno označit zpracovávání údajů, co se týče školení o právních předpisech ohledně zajištění bezpečnosti a ochrany zdraví při práci podle § 103 odstavec 2 a 3 zákoníku práce, nebo evidenci o distribuci hygienických prostředků podle § 104 odstavec 5 zákoníku práce.⁶²

Závěrem bych v této kapitole zmínil zpracovávání údajů státních zaměstnanců, kteří jsou ve služebním poměru. Jelikož se nejedná o klasický pracovní, ale služební poměr, nastávají zde jistá specifika. Jako osoby ve služebním poměru lze označit příslušníky Policie ČR, Hasičského záložního sboru ČR, Celní správy ČR, Vězeňské služby ČR, Bezpečnostní informační služby a Úřadu pro zahraniční styky a informace a vojáky z povolání. Konkrétně se zpracováním osobních údajů zabývá zákon 361/2003 Sb.⁶³, který stanovuje v §202 podmínky nakládání s informacemi obsažených v osobním spisu, na rozdíl od zákoníku práce určuje například maximální možnou dobu existence na 50 let. Další právní předpis zabývající se ochranou osobních údajů je v souvislosti se

⁶¹ BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5., str. 179

⁶² BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5., str. 161

⁶³ Zákon číslo 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů

státní službou zákon 234/2014 Sb.⁶⁴

4.3 Zpracování osobních údajů po ukončení pracovního poměru

V závěrečné části čtvrté kapitoly bude diplomová práce pojednávat o zpracování osobních údajů po ukončení pracovního poměru, tedy za předpokladu, že pracovní poměr vzniknul účinností pracovní smlouvy, která byla rozvázána. Jakási šedá zóna vzniká od okamžiku rozvázání pracovní smlouvy a vyplacení poslední mzdy. V tomto časovém úseku může zachovávat osobní spis zaměstnavatele v komplexní podobě.

Je nutné si vymezit, jaké přesně údaje může správce po rozvázání pracovního poměru uchovávat. S odkazem na článek 6 odstavec 1 písmeno c) Nařízení je správce údajů oprávněn osobní údaje bývalého zaměstnance uchovávat, pokud mu tak stanoví právní předpisy a má tak zákonný důvod. V praxi se jedná o daňové zákony a zákony související s důchodovým a sociálním pojištěním⁶⁵. Dalším případem uchovávání osobních údajů po ukončení pracovního vztahu je v Nařízení článek 6 odstavec 1 písmeno f), kdy zaměstnavatel uchovává osobní údaje pro potencionální soudní spor, kdy dokumenty a informace uvedené ve spise mohou sloužit jako důkazy. Lhůty pro toto uchovávání zákon taxativně neupravuje, ÚOOÚ ve své rozhodovací praxi ale judikuje, že tato lhůta musí být přiměřená a bez zbytečného prodlužování uchování.

5 Praktické otázky v souvislosti s GDPR – monitoring zaměstnanců

V páté části bude diplomová práce pojednávat o praktických otázkách, se kterými je možné se v souvislosti s GDPR setkat. Jelikož zaměstnavatel může své zaměstnance monitorovat, jak bude popsáno v následujících podkapitolách, je nutné si stanovit, co je ještě v souladu s Nařízením a dalšími právními předpisy a jaké úkony už přesahují pravomoci zaměstnavatele v souvislosti se zásahem do soukromí jeho zaměstnanců. Tyto zavedené mechanismy slouží zaměstnavateli k zajištění své bezpečnosti. Bezpečnost definuje Navrátil jako *„stav, kdy riziko ohrožení života a zdraví lidí, majetku je omezeno na přijatelnou*

⁶⁴ Zákon číslo 234/2014 Sb., zákon o státní službě

⁶⁵ Zejména zákon č. 582/1991 Sb., zákon o organizaci a provádění sociálního zabezpečení a zákon č. 187/2006, o nemocenském pojištění

úroveň.“⁶⁶ Nejčastěji se bude jednat právě na stav ohrožení co se týče majetku, kdy se tedy dostane do jakési protiváhy zájem zaměstnancových osobních údajů a zájem zaměstnavatelova majetku. Z §316 odstavce 1 zákoníku práce vyplývá, že zaměstnavatelovi nevzniká jakékoliv omezení v rozhodnutí s ohledem udělení povolení na využívání prostředků zaměstnancem, nicméně sám je povinen se řídit zákonným základem.

5.1 Kamery na pracovišti

Fenoménem moderní doby se staly kamerové systémy, které zaměstnavatelovi slouží k účelu ochraně nějakého jeho zájmu. Tento zájem lze rozdělit na dvě varianty a to sice, že zaměstnavatel kamerovým systémem chrání objekt pracoviště (např. před krádeží), nebo dohlíží na bezpečnost zdraví svých zaměstnanců.

Provozu kamerových systému se v právní úpravě dotýká §316 odstavec 2 zákoníku práce, který zavazuje zaměstnavatele v „*nenarušování zaměstnancova soukromí na pracovišti jeho skrytým nebo otevřeným sledováním, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty, nebo kontrole listovních zásilek*“. Zaměstnavatel musí proto zvolit tu nejvhodnější techniku, jakožto i výběr místa, zabezpečení proti neoprávněnému přístupu a výběr osob, která budou moci disponovat s nahraným záznamem, která bude ku prospěchu předem stanoveného účelu. Tyto podmínky definuje také Nařízení v článku 32 a článku 25.⁶⁷ Není proto v této souvislosti možné instalace kamer v převlékárnách, WC, nebo jiných prostorách, kde by bylo narušeno nejrelevantnější soukromí zaměstnance.

V souvislosti Nařízením připadají v úvahu provozu kamerového systému pouze dva zákonné důvody, kterými zaměstnavatel může prostřednictvím kamerového systému údaje subjektu zpracovávat, jenž jsou uvedeny ve článku 6 odstavec 1 písmeno c), tedy zpracovávání údajů pro splnění právní povinnosti

⁶⁶ NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, str. 208

⁶⁷ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 206

(zde se ve vnitrostátní právní úpravě nabízí zákon č. 186/2016Sb.⁶⁸, zákon č. 307/2013Sb.⁶⁹ a zákon č. 181/2014Sb.⁷⁰) a nadále odstavec 1 písmeno f) – zpracování osobních údajů nezbytných pro účely oprávněných zájmů příslušného správce či třetí strany (zmíněný monitoring objektu pracoviště před potenciální krádeží), tento právní důvod s sebou nese podmínku nezbytnosti, tedy takovou, že využití tohoto důvodu nebude mít přednost před samotnými právy a svobodou subjektů, kde se nabízí test proporcionality. Daný účel a využití jednoho ze dvou uvedených důvodů má povinnost správce vždy doložit a obhájit si jej.⁷¹ S odkazem na výše uvedené je proto možno konstatovat, že primární účel instalace kamerového zařízení nemá být dohled nad výkonností zaměstnance.

Instalace kamerového systému zavazuje správce informovat pozorovaný subjekt, že je snímán, to platí i o třetích osobách (klient v kanceláři). Vhodnosti informování se věnuje článek 13 Nařízení, který zavazuje správce vybrat vhodnou formu podání informace. V praxi tak můžeme uvést příklad, že zaměstnavatel informuje zaměstnance při nástupu do zaměstnání, nebo předseda SVJ při domovní schůzi. Transparentnost kamerového zařízení je možné zpozorovat i v jeho označení, či vzhledu. Vhodné by proto bylo označení místa kamery upozorňující tabulí, nebo podání zřetelné informace snímanému subjektu, kde je kamera umístěna a jaké prostory zachycuje.

Doba uchování kamerových záznamů není zákonně vymezená a odvíjí se podle jeho účelu. Samotný záznam musí mít svůj důvod využití, například při vyžádání Policií ČR. V situaci, kdy kamera zachytí událost, kde by vzniklo podezření na spáchání trestného, nebo jinak společensky škodlivého trestného činu, má být tento záznam předán Policii ČR k následným procesním úkonům, jelikož pouze ona je oprávněna nahrávky dále šířit (např. na svých facebookových stránkách). Jako příklad chybného jednání tak lze uvést moment, kdy bude z parkoviště objektu pracoviště odcizen služební vůz a správce záznamu vyvěsí tuto nahrávku na internet s cílem identifikovat pachatele.⁷²

⁶⁸ Zákon č. 186/2016 Sb., zákon o hazardních hrách

⁶⁹ Zákon č. 307/2013 Sb., zákon o povinném značení lihu

⁷⁰ Zákon č. 316/2014 Sb., zákon o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

⁷¹ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 208

⁷² ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-

5.2 Monitoring emailové pošty zaměstnanců

Existence emailu u osoby lze označit v moderní době samozřejmost. Jinak tomu ale bude s ohledem na jeho profesní stránku, neboť ani zdaleka každý zaměstnavatel nevede služební elektronické adresy. V druhé podkapitole se tak bude diplomová práce zabývat aspekty kontroly zaměstnavatelem, v jakém měřítku a situacích jí může vykonat a kdy se naopak jedná o neoprávněný zásah do soukromí.

Nejprve je nutné zmínit výklad článku 13 Listiny⁷³, která přímo deklaruje skutečnost, že je zaručena ochrana listovního tajemství, tedy, že „*nikdo nesmí porušit listovní tajemství jiných písemností a záznamů at' již uchovávaných v soukromí, nebo zasílaných poštou, anebo jiným způsobem.*“ Stejně dává subjektu právní jistotu nenarušení listovního tajemství §182 trestního zákoníku.⁷⁴ S odkazem na §316 odstavec 1 zákoníku práce ale využití techniky poskytnuté zaměstnavatelem zavazuje zaměstnance tuto techniku využívat jen a pouze pro účely spojené s výkonem povolání.

Otázka kontroly firemního emailu zaměstnavatelem je tedy poměrně komplikovaná, neboť i při existenci emailu, který má sloužit především k vyřizování pracovních záležitostí, se na něj vztahuje listovní tajemství, tedy, že zaměstnavatel nemůže sledovat obsah korespondence, s výjimkou pouze pokud je zaměstnanec například v dlouhodobé pracovní neschopnosti, nebo na služební cestě bez přístupu k vyřizování emailů (v takovém případě se ovšem nabízí varianta automatické odpovědi s přesměrováním na zastupujícího kolegu) s tím, že nemůže otevírat korespondenci osobní povahy, která byla zaměstnancovi zaslána. Druhá věc ale je, jestli, pokud má do schránky přístup, do něj smí nahlédnout. S poukázáním na to, že zaměstnavatel má právo sledovat docházku a dodržování pracovní doby zaměstnanců, se proto ÚOOÚ přiklání k názoru, že ano. Nicméně by měl k uvedenému přistupovat v nejvyšší obezřetnosti a předem

80-7554-097-3. str. 213

⁷³ Listina základních práv a svobod

⁷⁴ Zákon 40/2009Sb., trestní zákoník

⁷⁵ BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5., str. 129

zaměstnance informovat. Lze tedy konstatovat, že v některých případech může monitorovat čas a četnost odeslaných emailů. Vhodné by ale bylo, pokud by na svůj záměr, na základě zásady transparentnosti, zaměstnance upozornil.⁷⁶ Dle ÚOOÚ⁷⁷ je ale nutné rozdělit emailovou adresu konkrétního subjektu (danielbudil@firma.cz) a obecný firemní email (info@firma.cz). V prvním případě, tedy pokud email je zaslán na adresu konkrétního subjektu, se jedná o soukromou korespondenci, jakožto i o osobní údaj. Obecný, nebo také ústřední firemní email slouží ke komplexní komunikaci firmy se třetí stranou a k přečtení tohoto emailu nebude oprávněn jen jeden konkrétní subjekt. Obdobná situace také nastává v okamžik, pokud je na pracoviště zasláná korespondence v listinné podobě. Zaměstnavatel je povinen, pokud jde o soukromý dopis jej zaměstnancovi předat a nesmí do něj nahlížet. To ale neplatí, pokud bude v hlavičce jako první uveden název firmy a následně až uvedeno „k rukám ...“. V takovém případě by se nejednalo o korespondenci soukromou, ale firemní.

5.3 Monitoring služebních telefonů

Do další sféry, kde zaměstnavatel kontroluje aktivity svých zaměstnanců je možné zařadit i monitoring služebních telefonů. Je nutné zmínit, že článek 13 Listiny⁷⁸ vztahuje listovní tajemství i na obsah hovorů a SMS zpráv. Proto tato kapitola bude věnována intenzivě kontroly nad služebními telefony (pevné linky, mobily) ze strany zaměstnavatele.

Existuje několik způsobů, jak provádět monitoring služebních telefonů. Jedním z nejčastějších je instalace software na telefonu, který umožňuje zaměstnavatelům sledovat všechny aktivity na zařízení. Tento software může být použit k monitorování telefonních hovorů, SMS, e-mailů, prohlížení aplikací a dalších funkcí telefonu. Další možností je použití služeb třetích stran, které nabízejí monitoring služebních telefonů. Tyto služby často umožňují zaměstnavatelům sledovat telefonní hovory, textové zprávy a umístění telefonu v reálném čase. Tyto služby mohou být také použity k omezení přístupu k určitým funkcím telefonu, jako jsou například sociální sítě nebo zábavní aplikace.

⁷⁶ tamtéž

⁷⁷ Stanovisko č. 2/2009

⁷⁸ Listina základních práv a svobod

Je logické, že služební telefon má plnit svoji funkci především pro vyřizování služebních záležitostí. Ve věci využívání služebního příslušenství, tedy věcí, které jsou zaměstnancovi zaměstnavatelem po dobu pracovního poměru zapůjčeny, jsou ale telefony využívány k soukromým záležitostem nejčastěji. Bylo by tedy vhodné už při předání služebního telefonu zaměstnanci sdělit, respektive vymežit hranice jeho používání (slouží pouze pro vyřizování služebních hovorů; nemá přístup k internetu; zákaz psaní soukromých SMS zpráv; atd...). Podle zákoníku práce dále zaměstnanec odpovídá zaměstnavateli za škodu, kterou mu způsobil zaviněným porušením povinností při plnění pracovních úkolů nebo v přímé souvislosti s tímto plněním⁷⁹. Je tedy možné si představit situaci, kdy zaměstnanec nedodrží stanovené pravidla, jedná neohospodárně a dopustí se tedy porušení pracovní kázně, za což může být sankcionován například sražením peněz ze mzdy, nebo udělením napomenutí.

Zaměstnavateli se bude jednat o to ochránit svůj majetek, v tomto případě služební telefon, před zneužitím, tedy o využívání telefonu ze strany zaměstnance k soukromým účelům. Jelikož, jak je zmíněno výše, může zaměstnanec využívat telefon, pokud nedojde k jiné dohodě, pouze ke služebním účelům. Může tak dojít k prověření, zda tomu tak doopravdy činí. K tomuto prověření má dle zákoníku práce zaměstnavatel i zákonný nárok. Zaměstnavatel nemůže v žádném případě kontrolovat obsah hovorů nebo SMS, jelikož se jedná o listovní tajemství, může ale například zkoumat telefonní čísla, které přišly s číslem služebního telefonu do styku. V tomto případě se bude jednat o shromažďování osobních údajů ze strany zaměstnavatele a bude jej regulovat Nařízení.

5.4 Monitoring služebních automobilů

V případě využití služebního automobilu a jeho ochranou před zneužitím a nebo odcizením slouží zaměstnavatelům k této činnosti zejména GPS lokátory. Monitoring služebního automobilu si v souvislosti s Nařízením lze vyložit dvěma způsoby a to sice podle článku 6 odstavec 1 písmeno f), kdy zaměstnavatel nepotřebuje souhlas zaměstnance k využívání GPS, neboť se jedná o oprávněný zájem. Takové sledování ale musí být v souladu se zásadou přiměřenosti, tedy,

⁷⁹ BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5., str. 132

pokud je účel takového sledování kontrola pracovní výkonnosti, kvalita poskytování služeb, nesmí být monitoring nepřetržitý. Jako příklad lze uvést kurýrní služby zásilkových společností. Jsou ale výjimky, že pokud existuje závažný důvod vzhledem k činnosti společnosti, může být sledování nepřetržitě. V praxi lze uvést příklad neustálého sledování při činnosti bezpečnostní agentury převážející finanční prostředky.

Druhým právním důvodem je článek 6 odstavec 1 písmeno a) Nařízení, jako který uvádí souhlas zaměstnance s využíváním automobilu pro soukromé účely i se zahrnutím GPS lokátoru, kdy bude v určitých intervalech zaznamenáván pohyb vozidla, neboť u uvedeného případu jde o benefit, kdy při neudělení souhlasu se zaměstnancem nijak nedotkne.⁸⁰

Otázka nastává, v jaké situaci dochází k samotnému zpracování osobních údajů ze strany zaměstnavatele. Je proto nutné vycházet ze stanoveného účelu, tedy je možné označit za zpracování osobních údajů situaci, kdy zaměstnavatel využívá GPS lokátor k získání informací o přesném pohybu auta a o zaměstnancích, kteří služební vůz využívají. V případě, pokud by zaměstnavatel monitoroval jiné údaje, jako například počet najetých kilometrů na vozidle, o zpracování osobních údajů by se nejednalo.⁸¹

Závěrem bych zmínil, že vedle zásady přiměřenosti, o které pojednává první odstavec této podkapitoly, je důležitá i zásada transparentnosti. Zaměstnavatel má tedy povinnost o existenci sledovacího zařízení v automobilu zaměstnance informovat a nesmí využít skryté sledování. V případě nesplnění své povinnosti se zaměstnavatel vystavuje riziku sankcí od dozorového úřadu.

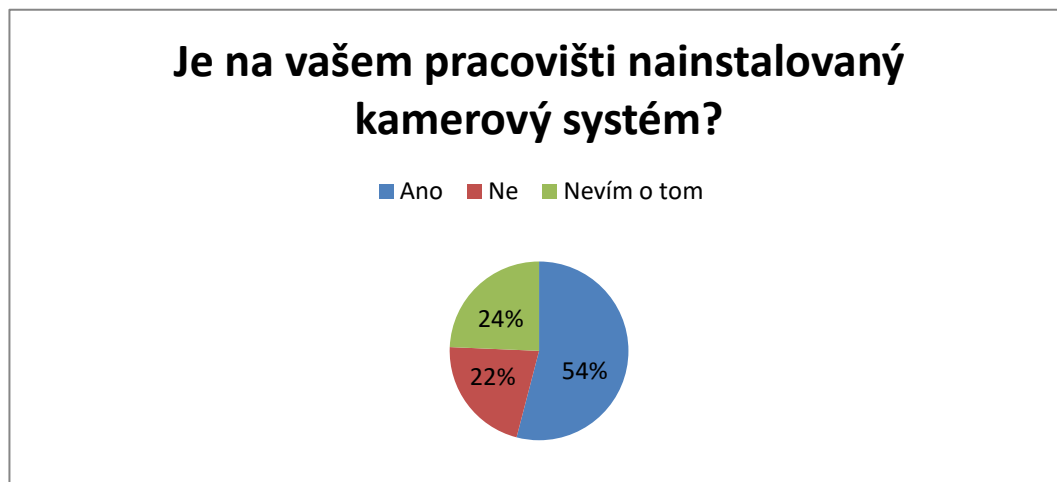
Dotazníkové šetření

V poslední části páté kapitoly bude prezentováno dotazníkové šetření, kterého se zúčastnilo 37 stejných náhodných respondentů, kde lze předpokládat, že místo výkonu práce budou vykonávat na jiné lokaci, kteří odpovídali na 5 otázek, které se týkaly právě hlavně tématům, kterým byl v této kapitole věnován

⁸⁰ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 71

⁸¹ BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5., str. 134

prostor. Dotazník byl koncipován po několika místech v Benešově u Prahy papírovou formou. Vždy bude nejdříve zobrazen graf s procenty, následně rozeberu výsledek s ohledem na fakta zmíněná v předchozích podkapitolách. Tedy:



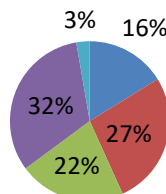
Graf 1

V první dotazníkové otázce 37 respondentů odpovídalo ohledně samotné existence kamerového systému na pracovišti. Tuto otázku jsem implementoval hlavně kvůli modernímu trendu instalace kamer na pracoviště, kde jsem očekával většinovou převahu výskytu na pracovišti, což 20 respondentů s 54% naplnilo. Celkem překvapivé bylo 9 respondentů, kteří neví, zda na pracovišti kamerový systém je, neboť by zaměstnavatel při jeho instalaci měl povinnost zaměstnance o přítomnosti systému dle Nařízení a zásady transparentnosti a zákonnosti informovat, jinak by se jednalo o skryté sledování, což je nezákonné. 8 odpovídajících ví, že při výkonu jejich povolání je kamerový systém nemonitoruje. Lze předpokládat, že to budou zaměstnanci, jejichž povolání může být ve venkovních prostorech (dělník, plynář, řidič, atd..).

Konečně lze tedy konstatovat, že odpovědi respondentů při této otázce byly očekávané, až na 9 odpovědi při volbě „nevím“, kde jsem očekával nižší hodnotu. Popularita kamerového systému ve vnitřních prostorech, jako jsou kanceláře nebo další provozovny roste, proto většinový výskyt dle odpovědi respondentů je možné označit za předpokládaný.

Sohlasíte (souhlasili byste) se zpracováním Vašich osobních údajů přes kamerový systém?

■ Rozhodně ano ■ Spíše ano ■ Rozhodně ne ■ Spíše ne ■ Je mi to jedno



Graf 2

Otázka číslo 2 monitoruje popularitu kamerového zařízení na pracovišti. Problematika kamerového systému s sebou nese i nepopularitu mezi zaměstnanci, neboť i při zákonném využití kamerového systému, pořád nějakým způsobem do soukromí zaměstnance na pracovišti zasahuje. Před vyhodnocením odpovědí u této otázky jsem očekával většinou nevoli s přítomností kamerového systému na pracovišti z důvodu popsaného v předchozí větě. Opět odpovídalo všech 37 respondentů. Výsledky pro mě byly více překvapující než u otázky číslo 1, neboť v celkovém počtu pro „ano“ 43% - 16 respondentů - (rozhodně ano 16%, spíše ano 27%), můžeme tento stav označit za lehce menšinový. Do výsledku je také možné přibrat fakt, že GDPR, je již v účinnosti od r. 2018, proto se jeho aplikace ze strany zaměstnavatele zdokonaluje a zpracování údajů je kamerovým systémem využíváno přesně podle zákona, i pod hrozbou vysokých pokut ze strany ÚOOÚ. 55% respondentů – 20 odpovědí - vybralo možnost „ne“ (22% rozhodně ne, 32% spíše ne, kde právě tato volba měla nejvíc hlasů). 1 respondent odpověděl, že mu to je jedno, kdy v návaznosti na celkem četný výskyt odpovědí v otázce číslo 1 pro možnost, že neví o přítomnosti kamer na pracovišti, lze pouze jednu odpověď označit za překvapivě nízkou.

Celkově je tedy možné udělat závěr, že moderní doba vyžaduje i zdokonalování a četnost moderního zařízení, jako jsou kamery. S tím se dle výsledků u této otázky vyvíjí i vnímání dané problematiky populací, kdy tato zařízení jsou více tolerována a jejich přítomnost čím dál tím více splývá s běžným životem. Pořád je dle odpovědí v malé většině ovšem možnost pro

nesouhlas s přítomností kamer na pracovišti, kvůli většímu nabourávání soukromí zaměstnanců ze strany zaměstnavatele.

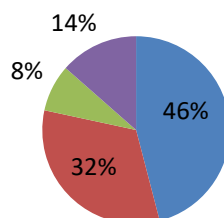


Graf 3

Další otázka v dotazníku se týkala zákonné povinnosti zaměstnavatele informovat své zaměstnance o zpracování osobních údajů na pracovišti před začátkem samotného zpracování. Výsledek skončil drtivou převahou s 92%, že zaměstnavatel svojí zákonnou povinnost dle GDPR splnil a řádně zaměstnance o monitoringu informoval. Tato otázka se netýkala pouze kamerového systému, ale celkového zpracování na pracovišti, proto je možné, že informování ze strany zaměstnavatele si někteří respondenti vyložili jako podepsání souhlasu se zpracováním osobních údajů dle GDPR, kde si ale troufnu tvrdit, že většina zaměstnanců tento souhlas nečte pro jeho obsáhlost, ale pouze jej podepíše. Zaměstnavatel ale tímto svoji povinnost samozřejmě splnil. Osobně jsem čekal převahu řádného informování zaměstnanců, nikoliv ovšem tak drtivou, kdy pouze 2 respondenti odpověděli, že nebyli informováni. Jak již bylo zmíněno ve třetí otázce, GDPR je již účinné delší dobu a zaměstnavatelé již dokáží jeho účel a své povinnosti aplikovat.

Domníváte se, že je momentální právní úprava GDPR ve vztahu k monitoringu na pracovišti dostačující?

■ Rozhodně ano ■ Spíše ano ■ Rozhodně ne ■ Spíše ne

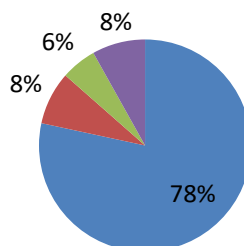


Graf 4

Další otázka se zakládala na subjektivním pocitu respondentů, jakým způsobem vnímají dostatečnost Nařízení ve vztahu k monitoringu na pracovišti. Celkem 78% - 29 respondentů (z toho 46% rozhodně ano a 32% spíše ano) odpovědělo, že se domnívá, že momentální úprava GDPR je dostačující a zakládá tak funkční a stabilní ochranu osobních údajů na pracovišti s ohledem na monitoring. Naopak méně než jedna čtvrtina (8 respondentů a 22%) si myslí, že momentální úprava dostačující není. Jelikož se jednalo o zaškrtačovací koncept dotazníku, nebyla zde možnost rozepsat svůj názor pro odůvodnění odpovědi. Z názorů odpovídajících je znát spokojenost s momentální úpravou GDPR.

Vnímáte z pohledu zaměstnance GDPR jako prospěšné? (ve srovnání s dobou před GDPR)

■ Rozhodně ano ■ Spíše ano ■ Rozhodně ne ■ Spíše ne



Graf 5

Pátá a tedy poslední otázka opět cílila na subjektivní pohled respondentů, tentokrát na samotné Nařízení jako předpis, který má chránit jejich osobní údaje a tedy práva a povinnosti spojené s nimi. Troufnu si říci, že doba pěti let od účinnosti GDPR v České republice je už takový úsek času, kdy lze udělat nějaký závěr. Otázka měla smysl právě v praktickém dopadu Nařízení při zaměstnání, neboť odpověď na otázku, zda-li je (nebo má být) GDPR pro zaměstnance prospěšné, tak je logicky, že ano. Toto šetření mělo spíše za úkol porovnat dobu před a po GDPR, tedy, jestli zaměstnanci v nějakém úhlu pohledu pocítili GDPR jako svůj benefit. Z 37 respondentů odpovědělo 86% - 32 osob (z toho 78% rozhodně ano a 8% spíše ano), že vnímají GDPR z pohledu zaměstnance jako prospěšné a GDPR tedy plní svoji funkci. Na druhé straně pouhých 14% - 5 respondentů uvedlo do dotazníku, že GDPR prospěšné z pohledu zaměstnance není.

U poslední otázky jsem očekával většinou převahu u odpovědí, že GDPR prospěšné pro zaměstnance je. Nutno podotknout, že u této otázky byla největší shoda ze všech u odpovědí (pokud bereme 4 odpovědi u otázky) a to, že se 78% respondentů shodlo, že rozhodně berou GDPR z pohledu zaměstnance jako přínos s ohledem na dobu před rokem 2018. Nutno podotknout, že nástup Nařízení s sebou přinesl velkou pozornost, což bývá dáváno za vinu velké míře nepřipravenosti na implementaci do vnitrostátního právní řádu, jakožto i nepřipravenost dozorového úřadu a vše se šilo tzv. „horkou jehlou“ a změn bylo hodně najednou. Celkové názory respondentů na GDPR lze tedy označit za kladné.

6 Rozhodovací praxe Úřadu pro ochranu osobních údajů

V šesté kapitole bude diplomová práce pojednávat o činnosti dozorového úřadu v České republice, který má název Úřad pro ochranu osobních údajů a to prakticky pro jakékoliv zpracování osobních údajů. Jeho koncept, působnosti a podmínky pro členy stanovuje zákon o zpracování osobních údajů⁸². Z Nařízení jako takového nevyplývá, zda členský stát musí zřídit pouze jeden dozorový úřad, nebo jich může mít více. Vzhledem ke konceptu České republiky je ale nepředstavitelné, že by zde působilo více dozorových úřadů, jako je tomu například v některých členských státech, které mají federativní charakter.⁸³

Nezávislost

Velmi důležitým aspektem dozorového úřadu je jeho nezávislost. Už od začátku mezinárodních právních předpisů v oblasti ochrany osobních údajů se považuje nezávislost dozorového úřadu za klíčový prvek účinného prosazování ochrany osobních údajů. Tuto nezávislost garantovaly Úmluva č. 108 a dodatečný protokol k ní, stejně jako směrnice 95/46/ES. S otázkou nezávislosti dozorových úřadů se zabývá Soudní dvůr Evropské unie.⁸⁴

Podle teorie správního práva má nezávislost správního úřadu tři základní složky: funkční, materiální (finanční) a personální. Tyto prvky jsou také obsaženy v komentovaném ustanovení Nařízení. První a druhý odstavec se týkají funkčního prvku nezávislosti a zajišťují svrchovaný výkon přidělených pravomocí. Třetí a částečně čtvrtý a šestý odstavec upravují materiální prvek nezávislosti. Personální prvek je popsán ve čtvrtém a zejména v pátém odstavci. V návaznosti s personálním prvkem je nutné si určit strukturu ÚOOÚ.

Obsazení ÚOOÚ

V Nařízení je rozlišováno mezi členy dozorového úřadu, jejichž jmenování,

⁸² Zákon č. 110/2019 Sb., zákon o zpracování osobních údajů

⁸³ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 353

⁸⁴ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 355

kvalifikaci a odvolání upravuje komentované ustanovení, a zaměstnanci tohoto úřadu. Mezi členy úřadu patří například předseda nebo další politicky jmenovaní zaměstnanci jako jsou inspektoři. Je na členských státech, jakým způsobem budou členy dozorového úřadu jmenovat, ať už prostřednictvím vlády, zákonodárského sboru, hlavy státu nebo jiných nezávislých subjektů, jako jsou soudy nebo profesní komory. V současné době je předseda a inspektoři ÚOOÚ voleni Senátem a jmenování prezidentem, což je v souladu s požadavky Nařízení.⁸⁵ V čem se ale liší česká právní úprava, tedy Zákon o zpracování osobních údajů od požadavků Nařízení je oblast kvalifikačních předpokladů pro předsedu a inspektory dozorového úřadu. Zákon požaduje pouze způsobilost k právním úkonům, bezúhonnost, negativní lustrační osvědčení a vysokoškolské vzdělání, zatímco Nařízení vyžaduje také zkušenosti a dovednosti v oblasti ochrany osobních údajů. Nařízení má za cíl zajistit, aby dozorové úřady byly expertními, nikoli politickými úřady, a aby měli členové dozorového úřadu dostatečné znalosti a zkušenosti v oblasti ochrany osobních údajů. Nicméně, alespoň nejvyšší představitel, tedy předseda, by měl zohledňovat i další celospolečenské zájmy.⁸⁶

Nařízení rovněž upravuje možnost odvolání člena dozorového úřadu z důvodu závažného pochybení při výkonu funkce. Důvodem pro odvolání by tam nemělo být například zaujetí odlišného výkladu, než v konkrétním případě zaujímají ostatní členové nebo který následně přijme správní soud, ale spíše pochybení ve smyslu nerespektování ustálené rozhodovací praxe dozorového úřadu či správních soudů, opakované průtahy v řízení atd.⁸⁷

Lze tedy konstatovat, že Nařízení přináší přísnější požadavky na kvalifikaci a zkušenosti členů dozorového úřadu, aby se zajišťovala kvalita ochrany osobních údajů, a upravuje i možnosti odvolání členů dozorového úřadu z důvodu závažného pochybení při výkonu funkce.⁸⁸

⁸⁵ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 356

⁸⁶ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 355

⁸⁷ tamtéž

⁸⁸ tamtéž

Příslušnost

Článek 55 GDPR stanoví, že národní dozorový úřad má pravomoc dohlížet na činnost správců a zpracovatelů osobních údajů, tedy zaměstnavatelů, kteří působí na území daného státu, pokud zpracování údajů probíhá v souvislosti s činností provozovny na území EU, bez ohledu na to, zda se zpracování samotné fyzicky odehrává mimo EU. To znamená, že pokud provozovna provádí činnost, která vyžaduje místní příslušnost podle článku 3 Nařízení, bude se dozorový úřad této země vztahovat na tuto provozovnu. Články 56, 60 Nařízení upravují spolupráci mezi dozorovými úřady při přeshraničním zpracování osobních údajů. Princip vedoucího dozorového úřadu se neuplatní, pokud se jedná o zpracování s přeshraničním prvkem, které je nezbytné pro plnění právní povinnosti správce, nebo pokud správce plní úkol ve veřejném zájmu nebo zpracování provádí při výkonu veřejné moci. Nově Nařízení vylučuje činnost soudů při výkonu soudních pravomocí z působnosti dozorových úřadů. Pokud by totiž dozorový úřad zasáhl do této činnosti, mohl by narušit nezávislost soudů a dělbu moci ve státě. Nicméně toto ustanovení nevyjímá soudy jako takové ze zpracování osobních údajů.⁸⁹

6.1 Úkoly dozorového úřadu

V první podkapitole se práce bude věnovat samotným úkolům dozorového úřadu. Jeho elementárním úkolem ve vztahu k Nařízení je dodržování funkčnosti, tedy zájem na ochraně základních práv a svobod fyzických osob v souvislosti zpracováním jejich osobních údajů.⁹⁰ ÚOOÚ má v porovnání s některými zahraničními úřady již podle stávající úpravy poměrně široké úkoly a kompetence. Nové úkoly mu však budou uloženy díky novým procesům a postupům, které Nařízení zavádí. Těmito úkoly jsou například posouzení vlivu na ochranu osobních údajů dle článku 35 Nařízení, nebo vydávání osvědčení podle článku 42 Nařízení. Úřad musí při plnění každého úkolu postupovat podle příslušných procesních předpisů, jako je správní a kontrolní řád.

Úkoly, které jsou ÚOOÚ ukládány, a jenž jsou taxativně vymezeny v článku

⁸⁹ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 361

⁹⁰ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 166

54 odstavce 1 Nařízení, lze rozdělit na šest kategorií. První zahrnuje obecnou povinnost sledovat uplatňování Nařízení a přispívat k němu. Druhou kategorií jsou úkoly spojené s edukací odborné i laické veřejnosti. Třetí kategorie se týká dozoru v užším smyslu. Čtvrtou kategorií jsou úkoly týkající se mezinárodní spolupráce. Pátou jsou úkoly týkající se konkrétních institutů či procesů a šestá kategorie zahrnuje všechny ostatní úkoly. Správci a zpracovatelé osobních údajů jsou povinni s dozorovým úřadem spolupracovat při plnění jeho úkolů, ale tato povinnost musí být vykládána proporcionalně.⁹¹ Je důležité také zmínit, že „provádění úkolů dozorového úřadu je pro subjekty údajů a pověřence bezplatné.“⁹² Pokud by nastala situace, že by nároky na dozorový úřad byly zjevně nedůvodné nebo by vybočovaly z jeho kompetencí pro jejich opakování, může dozorový úřad žadateli uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Poté by to musel dozorový úřad řádně zdůvodnit.⁹³

6.2 Pravomoci dozorového úřadu

Článek 58 Nařízení se zabývá pravomocemi dozorového úřadu, který má za úkol dohlížet na správné zpracování osobních údajů. Nařízení neposiluje současné pravomoci českého dozorového úřadu, ale upravuje nové kompetence, které se týkají například ohlašování případů porušení zabezpečení osobních údajů. Dozorový úřad bude moci využívat audit jako formu vyšetřování, který se zaměří na zjištění skutečného stavu při zpracování osobních údajů.⁹⁴

Další kompetencí je možnost dozorového úřadu hlásit správci nebo zpracovateli údajné porušení Nařízení, pokud získá indicii o porušení pravidel. Tato možnost není formálně upravena v právních předpisech, ale dozorový úřad již nyní postupuje podobným způsobem například v případech stížností na nevyžádaná obchodní sdělení. Celkově lze říci, že kompetence dozorového úřadu v souvislosti s Nařízením se zaměřují na posílení jeho pravomocí v oblasti nových právních institutů a umožňují u lépe dohlížet na správné zpracování

⁹¹ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 366

⁹² ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 168

⁹³ tamtéž

⁹⁴ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 368

údajů.⁹⁵

Důležitým faktem je, že i když Nařízení upravuje úkoly a pravomoci dozorového úřadu, tak ten musí vždy jednat s vnitrostátními předpisy. Lze etdy konstatovat, že konkrétní kroky, které dozorový úřad podnikne vůči správcům, zpracovatelům a dalším osobám, musí být v souladu s vnitrostátními procesními pravidly. Bod 129 odůvodnění Nařízení stanovuje základní zásady, kterými by se dozorový úřad měl řídit při výkonu svých úkolů, jako jsou například nestrannost, spravedlnost, hospodárnost a jednání bez zbytečných průtahů. Tyto všechny zásady jsou ale již obsaženy ve vnitrostátních předpisech, jako například v druhé hlavě správního řádu⁹⁶. Nelze proto vyvozovat nějakou větší změnu, než tomu bylo před účinností Nařízení.⁹⁷

Obecně lze pravomoci ÚOOÚ rozdělit na tři kategorie, jsou jimi vyšetřovací, nápravná, povolovací a poradní.⁹⁸ Tato podkapitola jednotlivě rozebere každou z nich.

Vyšetřovací pravomoc

ÚOOÚ bude při své vyšetřovací pravomoci využívat zejména právní předpisy kontrolní řád a správní řád.⁹⁹ Do Nařízení zákonodárce zařadil jak *obecné zmocnění ke kontrole zpracování osobních údajů ve článku 58 odstavec 1 písmeno b) Nařízení a ke kontrole ve vztahu k osvědčení ochraně údajů či pečeti a známek dle článku 42 Nařízení, tak následně jednotlivé kompetence týkající se získávání podkladů a informací nezbytných k individuálnímu dozoru ve článku 58 odstavec 1 písmeno a), e) a f).*¹⁰⁰ Komentované ustanovení zahrnuje pravomoci dozorového úřadu týkající se kontroly zpracování osobních údajů,

⁹⁵ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 368

⁹⁶ Zákon 500/2004Sb., správní řád

⁹⁷ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 368

⁹⁸ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 168

⁹⁹ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 169

¹⁰⁰ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 369

osvědčení o ochraně osobních údajů a získávání informací nezbytných pro individuální dohled. Tyto pravomoci jsou již zahrnuty v kontrolním řádu a neukládají žádné nové povinnosti pro správce nebo zpracovatele osobních údajů. Pokud jsou příslušné procesní předpisy svoji úpravou omezeny, jako je například základ vstupu do obydlí člověka, neplatí tak pro kontrolu podle tohoto Nařízení. Nicméně omezení z jiných procesních předpisů, jako je například §85 písmeno b) trestního řádu¹⁰¹, který se týká provádění domovní prohlídky nebo prohlídky prostor, ve kterých advokát vykonává advokacii, se vztahuje i na dozor prováděný podle tohoto Nařízení.¹⁰²

Žůrek tyto vyšetřovací pravomoci rozděluje do šesti možností:

- a) *Narídit správci a zpracovateli poskytnout veškeré informace, které jsou potřebné k plnění jeho úkolů,*
- b) *Provádět vyšetřování formou auditů ochrany údajů,*
- c) *Provádět přezkum vydaných osvědčení,*
- d) *Ohlásit správci nebo zpracovateli údajné porušení Nařízení*
- e) *Získat od správce a zpracovatele přístup ke všem osobním údajům a informacím, které potřebuje k výkonu svých úkolů,*
- f) *Získat přístup do všech prostor, v nichž správce a zpracovatel působí, včetně veškerého zařízení určeného ke zpracování osobních údajů.¹⁰³*

Nápravné pravomoci

V Nařízení je také řešeno možnost udělení nápravných opatření a sankci ze strany ÚOOÚ. Tato opatření mohou zahrnovat například povinnost poskytnout informace o zpracování osobních údajů, nařídit správci nebo

¹⁰¹ Zákon 141/1961 Sb., trestní řád.

¹⁰² NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 369

¹⁰³ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 168,169

zpracovateli, aby zpracování osobních údajů bylo v souladu s právní úpravou, omezit nebo zakázat zpracování osobních údajů nebo nařídít zastavení předávání osobních údajů do třetí země. Dozorový úřad má také pravomoc udělit správci nebo zpracovateli napomenutí, pokud dojde k porušení Nařízení, a může udělit sankční opatření. Při ukládání takových opatření se musí ÚOOÚ řídit zásadou proporcionality a zohledňuje všechny okolnosti případu.¹⁰⁴

Žůrek vymezuje deset takových pravomocí:

- a) *Upozornit správce či zpracovatele, že zamýšlená zpracování pravděpodobně porušují Nařízení*
- b) *Udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily Nařízení,*
- c) *Nařídít správci nebo zpracovateli vyhovět žádostem subjektu údajů při výkonu jeho práv,*
- d) *Nařídít správci nebo zpracovateli uvedení zpracování do souladu s Nařízením, případně stanovit i způsob a lhůtu,*
- e) *Nařídít správci, aby subjektu údajů oznámil porušení zabezpečení osobních údajů,*
- f) *Uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu,*
- g) *Nařídít opravu či výmaz osobních údajů nebo omezení zpracování a ohlašování těchto opatření příjemcům, kterým byly osobní údaje zpřístupněny,*
- h) *Odebrat osvědčení nebo nařídít, aby jej subjekt pro vydávání osvědčení odebral nebo aby jej nevydal, pokud nejsou plněny nebo již přestaly být plněny nebo již přestaly být plněny požadavky na osvědčení,*

¹⁰⁴ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 370

- i) *Uložit pokutu podle článku 83 Nařízení vedle či namísto nápravných opatření podle okolností každého jednotlivého případu,*
- j) *Nařídit přerušlení toků údajů příjemci do třetí země.¹⁰⁵*

Sankce a podmínky ukládání pokut

V každé právní normě obvykle existuje sankční část, která má za úkol donutit adresáty dodržovat pravidla stanovená normou. Nařízení není výjimkou a stanoví podmínky pro ukládání pokut za jeho porušení, včetně možné výše pokuty. Maximální výše pokuty za porušení GDPR je pro mnoho správců zdrojem velké pozornosti, protože se pohybuje až v milionech EUR. Nejvyšší možná peněžitá pokuta za porušení Nařízení je *20 000 000 EUR, jedná-li se o podnik, až do výše 4% celkového ročního obrátu celosvětově, podle toho jaká hodnota je vyšší, teoreticky tedy není horní hranice možné pokuty přesně stanovena, což se týká pouze podniku, kterým se podle definice v článku 4 odstavec 18 Nařízení rozumí jakákoliv fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost.* Tento předpis se tedy vztahuje na subjekty v celé Evropské unii a v extrateritoriálních situacích, což zahrnuje i některé světové společnosti. Velké pokuty jsou tedy v této oblasti na místě a mají preventivní a odstrašující funkci.¹⁰⁶

Povolávací a poradní pravomoci

Povolávací a poradní pravomoci ÚOOÚ, které jsou pospány v článku 58 odstavci třetím Nařízení, lze rozdělit do dvou skupin. První skupina zahrnuje pravomoci týkající se institutů, které Nařízení upravuje, jako je poskytování poradenství správci vztahujícího se k institutu předchozí konzultace, schvalování kodexů chování, akreditace subjektů vydávajících osvědčení a vydávání nebo schvalování kritérií pro jejich distribuci.

Druhá skupina se týká úpravy předávání osobních údajů mimo Evropskou

¹⁰⁵ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 170

¹⁰⁶ ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3. str. 178

unii, jako je schvalování smluvních doložek, správních ujednání a závazných podnikových pravidel. Dozorový úřad může také poskytovat stanoviska ohledně ochrany osobních údajů parlamentu a vládě na základě vlastního podnětu nebo vyžádání. Tyto pravomoci nahrazují obecnou konzultační povinnost, kterou měl dozorový úřad v minulosti. Dosavadní přístup při poskytování ze strany ÚOOÚ, kdy tak činí bez omezení, je považován odborníky za dobrou praxi.¹⁰⁷

Případy kontroly ÚOOÚ z praxe

V další části šesté kapitoly bude diplomová práce rozebírat jednotlivé reálné případy kontroly ÚOOÚ ve sféře pracovního práva, včetně jejich zjištění a výsledku.

Případ 1 – Kontrola zveřejňování fotografií zaměstnanců na internetových stránkách zaměstnavatele (ÚOOÚ-03225/2019)

ÚOOÚ zahájil kontrolu na základě stížnosti zaměstnankyně státní příspěvkové organizace, která se týkala zveřejnění fotografie stěžovatelky na internetových stránkách zaměstnavatele – kontrolované osoby. Úřad tedy rozhodl o zahájení kontroly na základě podané stížnosti a shromážděných podkladů od zaměstnankyně. V první fázi kontrolovaná osoba tvrdila, že má ve zveřejnění fotografie zaměstnankyně právní základ, kvůli jejímu souhlasu, která ovšem toto tvrzení označila za lživé, neboť žádný údajný souhlas nikdy neudělila a nadále požadovala výmaz její fotografie. Načež zaměstnavatel změnil svojí výpověď, kdy už tvrdil, že fotografie není na internetových stránkách umístěna z důvodu souhlasu zaměstnankyně, ale odkazu na oprávněný zájem kontrolované osoby ve smyslu článku 6 odstavce 1 písmeno f) Nařízení. Následně byl proveden balanční test z důvodu vyžádání zaměstnankyně, který konstatoval, že právní základ dle článku 6 odstavce 1 písmeno f) Nařízení zaměstnavateli neschází a umístění fotografie zaměstnankyně na internet bylo tedy nezákonné.

Dle provedené kontroly proto dospěl ÚOOÚ k závěru, že s ohledem

¹⁰⁷ NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 370

k výsledku balančního testu a k průběhu řízení, kdy zaměstnavatel změnil své původní výpovědi a nebyly tak důvěryhodnosti, bylo porušeno ze strany zaměstnavatele Nařízením dle článku 5 odstavec 1 písmeno a), z důvodu porušení zásady transparentnosti a zákonnosti. Kontrolovaná osoba následně podala k výsledku šetření námitky, z důvodu údajných procesních vad, které byly ovšem předsedou ÚOOÚ zamítnuty v plném rozsahu.¹⁰⁸

Případ 2 – Kontrola zpracování osobních údajů bývalých zaměstnanců (společnost Randstad s.r.o.)

Na základě stížnosti bývalého zaměstnavatele byla zahájena kontrola firmy Randstad – kontrolované osoby ze strany dozorového úřadu. Stížnost byla založena na údajném porušování Nařízením z důvodu, že společnost po rozvázání pracovního poměru se zaměstnancem ihned nezrušila firemní email, ba naopak do něj stále měla přístup, který využívala a z tohoto mělo vyplývat porušení soukromí a zpracování osobních údajů v rámci Nařízením. Ze stran kontrolujících bylo zjištěno, že emailová schránka je upravena vnitřními předpisy a nadále má společnost nastaveno bezpečnostní dodržování integrity e-mailového systému a schránek, které jsou v souladu s článkem 24 a 32 Nařízením. Argumentace kontrolované osoby dále obsahovala tvrzení, že emailová adresa existuje po rozvázání pracovního poměru ještě tři měsíce s nastavenou automatickou odpovědí s informací, že zaměstnanec již ve společnosti nepracuje a odkazem na jinou kompetentní osobu.

Dle zmíněného rozhodl ÚOOÚ, že nebylo v žádném ohledu porušeno Nařízením, respektive povinnosti, které z něj pro zaměstnavatele plynou i po ukončení pracovního poměru. Nebyl tedy porušen článek 30 ani 32 Nařízením a stížnosti tak nebylo vyhověno.¹⁰⁹

Případ 3 – Kontrola zpracování osobních údajů bývalých zaměstnanců (společnost 42 Financial Services a.s.)

¹⁰⁸ Kontrola zveřejňování fotografií zaměstnanců na internetových stránkách zaměstnavatele (ÚOOÚ-03225/19). *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/kontrola-zverejnovani-fotografii-zamestnancu-na-internetovych-strankach-zamestnavatele-uoou-03225-19/ds-6474/archiv=0&p1=6243>

¹⁰⁹ Kontrola zpracování osobních údajů bývalých zaměstnanců (společnost Randstad s.r.o.). *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-byvalych-zamestnancu-spolecnost-randstad-s-r-o/ds-5709/archiv=0&p1=5649>

Třetí rozebíraný případ činnosti ÚOOÚ se bude věnovat kontrole z důvodu stížnosti bývalého zaměstnance, který ve stížnosti uváděl jako rozpor s Nařízením dodržování práv subjektu údajů při vyřizování žádosti o přístup k osobním údajům dle článku 15 Nařízení. Po ukončení pracovního poměru se na svém bývalém zaměstnavateli stěžovatel domáhal přístupu k osobním údajům, čemuž společnost 42 Financial Services a.s., vyhověla pouze částečně a i při opakovaném naléhání stěžovatele o doplnění informací, které se týkaly jeho osobních údajů, nebylo tomu ze strany zaměstnavatele vyhověno a tyto žádosti ignoroval. Dále stěžovatel zmínil, že se mu nedostalo odpovědi o konečném příjemci osobních údajů.

Kontrolou ÚOOÚ bylo po prozkoumání všech důkazů a skutečností zjištěno, že ze strany zaměstnavatele bylo porušeno Nařízení ve svém článku 15 odstavec 1 písmeno c), *neboť v návaznosti na žádost subjektu je v zásadě nezbytné poskytnout informaci o konkrétních příjemcích osobních údajů*. Dozorový úřad dále rozhodl, že nebylo ve smyslu Nařízení porušeno poskytnutí přístupu bývalému zaměstnancovi o svých osobních údajích, neboť při doplnění požadovaných informací by se ke stěžovateli dostaly osobní údaje subjektů třetích stran, ke kterým neměl stěžovatel zákonný důvod. Všechny námitky byly předsedou ÚOOÚ zamítnuty.¹¹⁰

¹¹⁰ Kontrola zpracování osobních údajů bývalých zaměstnanců (společnost 42 Financial Services a.s.). *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-byvalych-zamestnancu-spolecnost-42-financial-services-a-s/ds-5731/archiv=0&p1=5653>

7 Judikatura

V sedmé kapitole bude rozebírána judikatura v souvislosti s ochranou osobních údajů a GDPR v pracovním právu. Budou představeny judikáty, které se týkají věcí, které diplomová práce postupně rozebírala. Jelikož Nařízení v mnoha směrech navazuje, ba i kopíruje směrnici 95/46/ES, jsou rozhodnutí soudů v některých případech relevantní i nyní, i když Směrnice byla Nařízením zrušena. Budou proto vybrány takové judikáty, kdy argumentace Směrnicí bude přípustná.

Věcná působnost – Rozsudek Soudního dvora ze dne 10. 7. 2018, *Jehovan todistajat*, C -25/17, Rozsudek Soudního dvora ze dne 6. 11. 2003, *Lindquist*, C-101/01, Rozsudek Soudního dvora ze dne 11. 12. 2014, *Ryneš*, C-212/13

V otázce věcné působnosti je klíčové rozdělit zpracování osobních údajů, na které se Nařízení vztahuje (tedy pozitivní vymezení), a na které nikoliv (negativní vymezení). Při rozdělení pozitivního vymezení je dále možné rozčlenit zpracování na automatizované a neautomatizované. Automatizovaným se rozumí zpracování osobních údajů za pomoci výpočetní techniky, při neautomatizovaném je takové zpracování prováděno výhradně lidmi bez použití techniky.

V rozsudku *Lindquist*, C-101/01 se Soudní dvůr vyjádřil na základě podnětu vnitrostátního švédského trestního soudu, který přerušil řízení, aby se dotázal Soudního dvora v otázkách výkladu „*zcela nebo částečně automatizované zpracování osobních údajů*.“ Řízení bylo vedeno z důvodu možného trestného činu paní Lidquist, která vytvořila internetové stránky, kde zveřejnila osobní údaje kolegů z farnosti. Na webových stránkách uvedla jejich jména, údaje o pracovním poměru či zálibách, rodinný stav, telefonní číslo a další informace včetně zdravotního stavu. V předběžné otázce bylo Soudním dvorem řešeno, zda zveřejnění těchto údajů se jedná o zcela nebo částečně automatizované zpracování osobních údajů. Soudní dvůr nejprve konstatoval, že „*pojem ‚zpracování‘ zahrnuje jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí, či bez pomoci automatizovaných postupů,*

mezi které patří také sdělení prostřednictvím přenosu, šíření nebo jakéhokoli jiného zpřístupnění.“ Poté ale dospěl k závěru, že zmíněné zpracování je třeba považovat „i úkon spočívající v uvedení osobních údajů na internetové stránce“. V této situaci, tedy že zveřejnění osobních údajů na webové stránky, vyžaduje připojení osob k internetu, které tak činí automatizovaně, jedná se o zpracování částečně automatizované.¹¹¹

Termín „automatizované zpracování“ byl klíčový také v Rozsudku Soudního dvora *Ryneš, C-212/13*, kdy Soudní dvůr konstatoval, že *„monitorování prostřednictvím obrazového záznamu zachycujícího osoby (...), ukládaného formou nekonečné smyčky do nahrávacího zařízení, a sice na pevný disk, přitom představuje v souladu s článkem 3 odstavec 1 směrnice 95/46/ES, automatizované zpracování osobních údajů.“*¹¹²

Při otázce neautomatizovaného zpracování, tedy při vedení evidence, které upravuje Nařízení v článku 4, bod 6 Nařízení, a definuje jej jako *„jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska“*, se Soudní dvůr zabýval v rozsudku *Jehovan todistajat, C-25/17*, kdy byla rozebírán spor mezi náboženskou skupinou Svědkové Jehovovi a dozorovým úřadem. V tomto případě byla klíčová definice „evidence“ a její výklad, tedy pokud se jí rozumí zpracování osobních údajů na bázi podomní kazatelské činnosti, kdy jsou zaznamenávány osobní údaje navštívených osob, včetně jejich jmen a adres, pro následné použití náboženskou skupinou. Dle Soudního dvora je nutné pojem evidence *„vykládat široce tak, že se vztahuje na ‚jakýkoli‘ uspořádaný soubor osobních údajů.“*, tedy i na tento případ. Nehraje proto roli, jakou má mít podobu, důležité je, aby shromážděné údaje měly ucelenou uspořádanou podobu a aby měly za účel jejich pozdější použití. Soudní dvůr tedy konstatoval, že evidencí takové zpracování osobních údajů je.¹¹³

¹¹¹ POKORNÁ, Andrea a Helena DVOŘÁKOVÁ. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek: stěžejní judikatura SDEU a vybraná judikatura ESLP : výkladové pokyny a stanoviska skupiny WP29 a EBDP : zákon o zpracování osobních údajů*. Praha: Wolters Kluwer, 2020. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-309-1, str. 34

¹¹² tamtéž

¹¹³ POKORNÁ, Andrea a Helena DVOŘÁKOVÁ. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek: stěžejní judikatura SDEU a vybraná*

Místní působnost – Rozsudek Soudního dvora ze dne 13. 5. 2014, Google Spain a Google, C-131/12

V první řadě je při otázce místní příslušnosti vymezení pojmu „provozovna“, kterou Nařízení definuje v článku 3 odstavec 1, kdy správce nebo zpracovatel má provozovnu na území členského státu EU. Nařízení se poté dále věnuje provozovně v návaznosti na zpracování osobních údajů a říká, že se vztahuje na každé zpracování probíhající v souvislosti s její činností, a to bez ohledu na to, zda zpracování probíhá v EU, nebo mimo ní.

V rozsudku *Google Spain a Google, C-131/12* byla řešena předběžná otázka místní působnosti Soudním dvorem, kterou mu položil španělský vnitrostátní soud ve věci pana Gonzáleze, který se dožadoval vymazání webové stránky z výsledků hledání na Googlu, jež obsahovala jeho osobní údaje. *Konkrétně bylo řešeno, zda je dána místní působnost směrnice 95/46/ES, která se svým výkladem „provozovna“ a „vykonávané v rámci činnosti provozovny“ neodchyluje od Nařízení, v případě, kdy provozovatel internetového vyhledávače (Google Inc.) zřídí v členském státě pobočku nebo dceřinou společnost určenou k podpoře prodeje a k prodeji reklamního prostoru nabízeného tímto vyhledávačem, která zaměřuje svou činnost na obyvatele tohoto státu (Google Spain).*¹¹⁴ Soudním dvorem bylo konstatováno, že Google Spain naplňuje definici podmínky provozovny, neboť skutečně a účinně vykonává činnost prostřednictvím stálého zařízení ve Španělsku a je pobočkou Google Inc. Na španělském území. *Rozhodující bylo, že činnost provozovatele vyhledávače a činnost takové provozovny byly neoddělitelně spojeny. Vzhledem k tomu, že při zobrazení seznamu výsledků vyhledávání prostřednictvím vyhledávače byla na stejné stránce zobrazena reklama spojená s vyhledávanými pojmy, bylo zpracování osobních údajů „prováděno v rámci reklamní a obchodní činnosti provozovny správce na území členského státu, v projednávané věci na španělském území.“*¹¹⁵

judikatura ESLP : výkladové pokyny a stanoviska skupiny WP29 a EBDP : zákon o zpracování osobních údajů. Praha: Wolters Kluwer, 2020. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-309-1, str. 35

¹¹⁴ Tamtéž, str. 36

¹¹⁵ POKORNÁ, Andrea a Helena DVORÁKOVÁ. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek: stěžejní judikatura SDEU a vybraná judikatura ESLP : výkladové pokyny a stanoviska skupiny WP29 a EBDP : zákon o zpracování osobních údajů.* Praha: Wolters Kluwer, 2020. Právní monografie (Wolters Kluwer ČR). ISBN

Osobní údaj – Nejvyšší správní soud České republiky sp. zn. 1 As 13/2011-210

Termínem osobní údaj je definováno v článku 4 bodu 1 Nařízení jako „*veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby*“, která je označována za subjekt údajů.¹¹⁶ V následujícím judikátu bude rozebrán případ, kdy se český nejvyšší správní soud zabýval případem, zda se o osobní údaj jednalo, či nikoliv.

V tomto případě šlo o to, že reportérka České televize Nora Fridrichová zveřejnila reportáž poukazující na údajně nevýhodné smlouvy mezi advokátní kanceláří Brož & Sokol & Novák a Dopravním podnikem hlavního města Prahy. Advokátní kancelář ve svém tiskovém prohlášení, kromě ohrazení se vůči reportáži podalo kritické vyjádření na adresu Fridrichové, kdy zveřejnila několik soudních rozsudků, které se týkaly jízdy „na černo“ osobou N.F. Nejvyšší správní soud se zabýval otázkou, zda zveřejnění soudních rozsudků bylo osobním údajem. Nakonec konstatoval, že identifikátory uvedené v rozsudcích, včetně jejich zveřejnění v reakci na odvysílanou reportáž, zpracování osobních údajů je.¹¹⁷

Souhlas se zpracováním osobních údajů – Rozsudek velkého senátu Soudního dvora ze dne 5. 10. 2004, Pfeiffer a další, C-397/01 až C-403/01

S ohledem na dřívější úpravu problematiky souhlasu směrnicí 95/46/ES zavádí Nařízení změnu v takovém ohledu, aby nešlo o pouhou formalitu, ale aby souhlas byl dle článku 4 odstavce 11 Nařízení jako „*svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává své svolení ke zpracování svých osobních údajů*“ a to buď formou prohlášení nebo zjevným a jasným potvrzením. Nařízení s sebou přineslo změny v definici, podmínkách udělení souhlasu a dále také v právním titulu zpracování na základě souhlasu. Lze tedy konstatovat, že Nařízení určuje přísnější podmínky než směrnice 96/46/ES, kdy například v článku 7 stanovuje pravidla pro udělení tohoto souhlasu a to včetně *požadavků na žádosti o jeho vyjádření a právo jeho*

978-80-7598-309-1, str. 38

¹¹⁶ Tamtéž, str. 9

¹¹⁷ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, str. 134

odvolání, které vysvětluje v recitálech 32,33,42 a 43.

V konkrétním judikátu *Pfeiffer*, se Soudní dvůr zabýval otázkou zda zaměstnanec při situaci, kdy vykonává pracovní dobu delší než 48 hodin týdně, musí udělit souhlas jednotlivě, svobodně a výslovně, nebo zda postačí odkaz v pracovní smlouvě na smlouvu kolektivní, která takovou alternativu umožňuje. Ačkoliv se v tomto případě nejedná přímo o souhlas, který zaměstnanec uděluje se zpracováním osobních údajů, je tento judikát důležitý pro představu formu souhlasu. Soudní dvůr tedy řešil otázku, zda kolektivní smlouva může být legitimní možností pro udělení souhlasu. V rozsudku bylo rozhodnuto, že ačkoliv je překročení pracovní doby 48 hodin týdně podle zákona možné, musí zaměstnanec takový souhlas vyjádřit individuálně, ale také výslovně a svobodně. V odůvodnění dále Soudní dvůr poznamenal, že „v tomto ohledu nepostačuje, aby pracovní smlouva dotčené osoby odkazovala na kolektivní smlouvu, která takové překročení umožňuje.“¹¹⁸

Správce, zpracovatel – Rozsudek Soudního dvora ze dne 5. 6. 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16

Při definici termínu „správce“ Nařízení zachovalo původní úpravu uvedenou ve směrnici 95/46/ES. Změny přineslo GDPR při upřesnění některých pojmů jako jsou společné správcovství, konkrétní požadavky na obsah zpracovatelské smlouvy, povinnost jmenovat zástupce správce nebo zpracovatele na území EU a řetězení zpracovatelů.¹¹⁹

Judikát ve věci *Wirtschaftsakademie Schleswig-Holstein, C-210/2016*, se týkal společnosti, která působila v oblasti vzdělávání a nabízela uživatelům sítě Facebook svůj produkt přes tuto platformu (jednalo se o vývoj vzdělávací činnosti), přes anonymní údaje. Administrátoři této stránky se ale dostali přes soubory cookies k datům uživatelů. Dozorový úřad proto nařídil tento produkt zrušit, neboť nebyl v souladu s ochranou osobních údajů uživatelů, protože nebyla dodržena informační povinnost ze strany společnosti.

¹¹⁸ Tamtéž, str. 80

¹¹⁹ POKORNÁ, Andrea a Helena DVOŘÁKOVÁ. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek: stěžejní judikatura SDEU a vybraná judikatura ESLP : výkladové pokyny a stanoviska skupiny WP29 a EBDP : zákon o zpracování osobních údajů*. Praha: Wolters Kluwer, 2020. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-309-1, str. 227

Wirtschaftsakademie argumentovala, že nemá kontrolu a ani nerozhoduje o zpracování osobních údajů, tedy, že nemá status správce, ale že tím je Facebook. Soudní dvůr argumentoval, že společnost Facebook Inc. sice určuje účely a prostředky zpracování, ale rovněž i administrátor stránky se na této činnosti podílí, neboť samotné založení stránky je důvod pro shromažďování a zpracování údajů (i když ne příliš osobního rázu, typu geografická poloha uživatele, preference, atd.). Soudní dvůr tedy rozhodl, že společnost Wirtschaftsakademie má status společného správce. Z uvedeného je proto zřetelné, že status správce je judikaturně vykládán široce, tedy označuje poměrně široké spektrum zúčastněných a stačí i „malá míra“ zpracování a shromažďování osobních údajů, aby dotyčný správcem byl.¹²⁰

Zpracování, shromažďování a uchovávání osobních údajů

Existuje mnoho způsobů, jak mohou být osobní údaje zpracovány. Nyní budou stručně rozebrány judikáty, kde Soudní dvůr rozhodl v podstatných případech. V Rozsudku Soudu prvního stupně ze dne 18. 2. 2004, *Esch-Leonhardt a další v. ECB*, T-320/02 rozhodl tak, že zařazení e-mailového dopisu týkajícího se zasílání odborových informací do osobních složek těm, kteří jej zaslali, znamená, že jsou osobní údaje ukládány do personálního evidenčního systému. Evropská centrální banka tedy zpracovávala osobní údaje tím, že je ukládala do personálního evidenčního systému, když zařadila dopisy týkající se přenosu informací odborů do osobních složek zaměstnanců elektronickou poštou.¹²¹

Podle rozsudku prvního stupně ze dne 12. 9. 2007, *Nikolaou v. Komise*, T-259/03 je naznačeno, že neoprávněné poskytnutí novináři tiskové zprávy, která obsahuje osobní údaje, je také považováno za zpracování osobních údajů.¹²²

¹²⁰ POKORNÁ, Andrea a Helena DVOŘÁKOVÁ. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek: stěžejní judikatura SDEU a vybraná judikatura ESLP : výkladové pokyny a stanoviska skupiny WP29 a EBDP : zákon o zpracování osobních údajů*. Praha: Wolters Kluwer, 2020. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-309-1, str. 227

¹²¹ Tamtéž, str. 31

¹²² POKORNÁ, Andrea a Helena DVOŘÁKOVÁ. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek: stěžejní judikatura SDEU a vybraná judikatura ESLP : výkladové pokyny a stanoviska skupiny WP29 a EBDP : zákon o zpracování osobních údajů*. Praha: Wolters Kluwer, 2020. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-309-1, str. 32

Soudní dvůr v Rozsudku ze dne 17. 10. 2013, *Schwartz*, C-291/12, bod 28-29 uvedl, že zpracování osobních údajů třetích osob zahrnuje jakýkoliv úkon s otisky prstů, jako je jejich sběr, záznam, uchování, konzultace nebo použití. Odebírání otisků prstů od osob a jejich uložení v paměťovém médiu cestovního pasu (ve sféře pracovního práva je možné si představit docházkový systém založený na otisku prstu) je považováno za zpracování osobních údajů.¹²³

Kvalifikace zaměstnance – Nejvyšší soud České republiky sp. zn. 21 Cdo 2305/2015

Další část judikaturní část se bude věnovat již kapitolám 4 a 5, tedy GDPR v jednotlivých fázích pracovního poměru a praktickým otázkám v souvislosti s GDPR. První judikát rozebere kvalifikaci zaměstnance v souvislosti s rozhodnutím Nejvyššího soudu České republiky, který upozorňuje, že to, zda zaměstnanec má kvalifikaci, neznamená pouze to, že má potřebné znalosti, dovednosti a zkušenosti pro výkon své stávající práce. Kvalifikace zaměstnance zahrnuje i schopnost vykonávat různé další pracovní činnosti, které zaměstnanec možná přímo nevykonává v rámci svého pracovního poměru. Pokud je práce vyžadující odbornou kvalifikaci, obvykle se k ní pojí i další činnosti, které nevyžadují zvláštní kvalifikaci. Práce odpovídající kvalifikaci zaměstnance znamená, že zaměstnanec může využít své získané kvalifikace v převážné míře, při čemž nevykonává práci, při které nemůže uplatnit svou kvalifikaci, a kterou by mohl vykonávat i pracovník s nižší kvalifikací, nebo bez ní.¹²⁴

Zákaz diskriminace – Nejvyšší soud České republiky sp. zn. 21 Cdo 4429/2013

Nejvyšší soud dále judikoval v souvislosti se zákazem diskriminace toliko, že jestliže došlo k porušení práv a povinností týkajících se rovného zacházení nebo diskriminaci v rámci procesu zaměstnávání (tedy v tomto případě před uzavřením pracovního poměru), není dostatečným opatřením, které by zaměstnavatel mohl přijmout, aby odstranil následky takového porušení nebo diskriminace, pouze přijetí daného zaměstnance do pracovního poměru. To

¹²³ tamtéž

¹²⁴ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, str. 342

znamená, že pokud zaměstnavatel odmítne zaměstnat osobu na základě porušení práv a povinností týkajících se rovného zacházení nebo diskriminaci, není to dostatečné vyrovnání se s tímto problémem.¹²⁵

Kamery na pracovišti – López Ribalda proti Španělsku (č. 1874/13)

Rozsudek López Ribalda proti Španělsku je rozhodnutí Evropského soudu pro lidská práva, který se týkal otázky, zda je způsob jakým zaměstnavatel instaloval kamery v souladu se zákonem. Konkrétně se jednalo o instalaci skrytých kamer na pracovišti, kdy zaměstnavatel podezříval některé zaměstnance v obchodním domě z krádeží a sledoval tak jejich pohyb na pracovišti. ESLP uznal ve svém rozsudku, že použití kamer bylo v souladu se zákonem a že zaměstnavatel tak chránil svůj majetek. Nicméně ESLP dále rozhodl, že zaměstnanci nebyli dostatečně informováni o instalaci kamer a sledování jejich pohybu na pracovišti a že jejich právo na soukromí bylo porušeno. ESLP dále také uvedl, že sledování mohlo být provedeno jiným způsobem, který by byl méně invazivní a byla tak narušena zásada přiměřenosti a transparentnosti. Právě rozsudek López Ribalda proti Španělsku je důležitým příkladem toho, jaké jsou limity použití sledovacích technologií na pracovišti. ESLP svým rozsudkem dal jasně najevo, že zaměstnavatelé mají povinnost informovat své zaměstnance o použití takových technologií a musí zajistit, aby bylo jejich právo na soukromí respektováno. Pokud tomu tak nebude, mohou být zaměstnavatelé odpovědní za odškodnění.

Monitoring emailové pošty zaměstnanců – Barbulescu proti Rumunsku (č. 61496/08)

V kauze Barbulescu proti Rumunsku se Evropský soud pro lidská práva zaobíral problematikou soukromí zaměstnance na pracovišti a přístupu zaměstnavatele k elektronické komunikaci svých zaměstnanců. Konkrétně se jednalo o případ rumunského zaměstnance, kterému byla dána výpověď za to, že používal firemní emailový účet k soukromé korespondenci. Zaměstnanec se bránil tím, že vyřizovaná korespondence byla pracovního rázu, zaměstnavatel ale jako důkaz předložil četnost emailů, koncové adresy a obsah korespondence.

¹²⁵ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, str. 342

ESLP v tomto případě rozhodl, že zaměstnavatel může sledovat elektronickou komunikaci svých zaměstnanců pouze tehdy, pokud je takové sledování nezbytné pro dosažení legitimního cíle a pokud je v souladu s právem na soukromí zaměstnanců. V případě konkrétního zaměstnance však zaměstnavatel není oprávněn sledovat všechny jeho emailové zprávy, včetně těch soukromých, pokud zaměstnanec nebyl o takovém sledování informován a nebyla mu poskytnuta možnost se proti němu bránit. V tomto případě byl zaměstnanec srozuměn se zákazem používání firemního emailu pro soukromé účely, nebyl však informován o jeho monitorování. ESLP také uvedl, že právo na soukromí platí i na pracovišti a že zaměstnanci mají právo na respektování svého soukromí, včetně jejich elektronické komunikace, pokud nejsou tato práva omezena oprávněnými důvody.¹²⁶¹²⁷

Monitoring služebních telefonů – Copland proti Velké Británii (62617/00)

Judikát Copland proti Velké Británii byl vynesena Evropským soudem pro lidská práva v roce 2007 a týkal se monitorování služebního telefonu zaměstnankyně paní Copland, která pracovala jako asistentka náměstka v Anglii a byl jí rozvázan pracovní poměr po tom, co byla zaměstnavatelem odhalena při zneužívání služebního telefonu k soukromým účelům. Paní Copland se odvolala k ESLP a tvrdila, že bylo porušeno její právo garantující respektování soukromí a rodinného života a listovního tajemství. Zaměstnavatel průběžně kontroloval korespondenci a výpis hovorů zaměstnankyně ze služebního telefonu za účelem zjištění, zda nedochází jeho využívání k soukromým účelům bez předchozího informování zaměstnankyně. Jelikož zaměstnavatel neměl konkrétní zákonný důvod ke sledování a nebyla tak zásada zákonnosti a transparentnosti, jelikož paní Copland neinformoval, ESLP rozhodl spor ve prospěch zaměstnankyně a přiznal jí odškodné 3000 €. ¹²⁸

¹²⁶ MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019, str. 388

¹²⁷ Barbulescu proti Rumunsku. *Eslp.justice.cz* [online]. Dostupné z: http://eslp.justice.cz/justice/judikatura_eslp.nsf/WebSearch/4C37F9ACAFF53B7AC125822E004D8EFF?openDocument&Highlight=0,

¹²⁸ Copland proti Velké Británii. *Ictjudikatura.law.muni.cz* [online]. Dostupné z: https://ictjudikatura.law.muni.cz/wiki/62617/00_-_Copland_proti_Velk%C3%A9_Brit%C3%A1nii

8 Zahraniční exkurz

V závěrečné kapitole diplomové práce budou zmíněny zajímavé případy týkající se ochrany osobních údajů v zahraničí.

Albánská prokuratura vyšetřuje únik osobních údajů 700 000 lidí, včetně premiéra

Albánská prokuratura provádí rozsáhlé vyšetřování ohledně úniku osobních dat více než 700 000 lidí včetně prezidenta a premiéra země. Informace, jako jsou zaměstnavatelé, mzdy a telefonní čísla byly zveřejněny na sociálních sítích, Média uvádějí, že byla odcizena data zaměstnanců bank, zaměstnavatelů, státních úředníků, členů rozvědky, armády a novinářů. Útok byl pravděpodobně proveden zevnitř s přístupem do databází osobních údajů, nikoli prostřednictvím kybernetického útoku. Premiér Edi Rama ujistil veřejnost, že situace bude státními orgány řádně prošetřena. Tento únik osobních údajů ale není v Albánii ojedinělý – v dubnu 2022 v podobném útoku došlo k úniku minimálně milionu obyvatel.¹²⁹

IKEA je ve Francii před soudem kvůli špehování svých zaměstnanců

Ve Francii v souvislosti s ochranou osobních údajů zaměstnanců probíhal soudní proces s bývalým vedením francouzské pobočky nábytkářské společnosti IKEA kvůli podezření z špehování vlastních zaměstnanců,. Firma IKEA jako právnická osoba a několik fyzických osob, včetně policistů a zaměstnanců bezpečnostní služby, čelilo obvinění z porušení soukromí zaměstnanců a získání a zpracování jejich osobních údajů bez jejich vědomí nebo souhlasu. Soud firmě uložil pokutu 1 milion € a generálnímu řediteli pobočky Jeana- Louise Baillotovi trest odnětí svobody v délce dvou let s podmíněným odkladem. Společnost si od bezpečnostní agentury nechávala prověřovat minulost a soukromí zaměstnanců bez jejich vědomí a zjišťovala informace o jejich politických a ekologických názorech.¹³⁰

¹²⁹ Albánská prokuratura vyšetřuje únik osobních údajů 700.000 lidí, včetně premiéra. *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/albanska-prokuratura-vysetruje-unik-osobnich-udaju-700-000-lidi-vcetne-premiera/ds-6914/archiv=0&p1=3938>

¹³⁰ IKEA špehovala zaměstnance, rozhodl francouzský soud. Má zaplatit milion

H&M zavře 250 obchodů. Navíc dostal obří pokutu za špehování

Německé dozorové úřady uložily firmě H&M pokutu ve výši 35,3 milionu € za sledování zaměstnanců v servisním centru v Norimberku, kvůli porušení GDPR. Jedná se tak o druhou světově historicky nejvyšší pokutu za existence Nařízení. Výše této pokuty má za cíl hlavně prevenci a odstrašit podobné porušení. Sledování stovek zaměstnanců bylo podle německého dozorového úřadu vedeno intenzivně a hrubě porušovalo zásady GDPR.¹³¹

eur. *Uoou.cz* [online]. Dostupné z: https://www.idnes.cz/ekonomika/zahranicni/ikea-soud-francie-pokuta-spehovani.A210615_112940_eko-zahranicni_mato

¹³¹ Řetězec H&M zavře 250 obchodů. Navíc dostal obří pokutu za špehování zaměstnanců. *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/retzec-h-amp-m-zavre-250-obchodu-navic-dostal-obri-pokutu-za-spehovani-zamestnancu/ds-6377/archiv=0&p1=3938>

9 Závěr

Cílem diplomové práce bylo čtenáři komplexně objasnit vliv GDPR na pracovní právo. V úvodní kapitole jsem se věnoval historickému formování ochrany osobních údajů, která se i vývojem moderních technologií a s tím i snazšímu přístupu k údajům se musí dále inovovat a stanovovat užší mantinely pro jejich úpravu, zpracování a získání. Takovým procesem se ochrana osobních údajů dostala až do vydání Obecného nařízení, které nabylo účinnosti 24. května 2018 a zrušilo předchozí směrnici 95/46/ES, která již nestíhala v některých aspektech stačit právě inovaci moderních technologií a jelikož se jednalo o směrnici, nenastala zde povinnost přímé právní závaznosti pro členské státy EU. Proto bylo nutné vydání jednotného právního předpisu, který bude přímo zavazovat jeho implementací členské státy EU. Pro pochopení smyslu GDPR bylo potřebné pochopit jednotlivé pojmy, které jej tvoří. Tomu se věnovala další kapitola teoretické části diplomové práce, která postupně ve svých podkapitolách rozebrala stěžejní termíny sféry ochrany osobních údajů. Dále jsem se věnoval nejdůležitějším zásadám, což je možné vnímat jako vůdčí ideje, v jejichž duchu se Nařízení nese a od kterých se nelze odchýlit, neboť by poté byla narušena samotná podstata právního předpisu.

Druhá, praktická část, nabídla čtenáři nejdříve rozbor zpracování osobních údajů v jednotlivých fázích pracovního poměru a objasnila, do jaké míry může zaměstnavatel podle Nařízení zaměstnancovy údaje zpracovávat s odkazem na jednotlivé praktické příklady. Zmínil jsem také důležitý aspekt zákazu diskriminace před nástupem do pracovního poměru, protože osobní údaj, jako je například pohlaví, nebo náboženství, může být pro zaměstnavatele potencionální překážkou pro přijetí zaměstnance. Určil jsem tak situace, ve kterých se zaměstnavatel pohybuje mezi a kdy za hranicemi práva. Poměrně velká část byla věnována osobnímu spisu zaměstnance, jelikož ho vnímám jako nejintenzivnější zpracování osobních údajů během pracovního poměru. Dále jsem uvedl další situace, kde je možné se se zpracováním osobních údajů na pracovišti setkat, jako je docházkový systém nebo otázka údajů o mzdě. Ač se může zdát, že při rozvázání pracovního poměru nemá mít zaměstnavatel se zaměstnancem od okamžiku vyplacení poslední mzdy nic společného a uplatní se zde právo zaměstnance „být zapomenut“ podle Nařízení, není toto tvrzení úplně pravdivé.

Tomu se věnuje rozbor poslední fáze pracovního poměru, tedy po ukončení zaměstnavatel může uchovávat osobní údaje zaměstnance sice pro taxativně zákonem uvedené případy, ale jisté zpracování stále probíhá.

V kapitole páté jsem se věnoval praktickým ukázkám monitoringu zaměstnanců na pracovišti s následným dotazníkovým šetřením, u kterého jsem položil 37 zaměstnancům, kteří pracují na rozdílných pracovištích, otázky, jenž se týkaly právě monitoringu. Za oblíbený a nejčastější monitoring zaměstnanců lze označit kamerový systém. Čtenářovi bude tak objasněno, za jakých předpokladů lze tento systém využít. Dále jsem se zaměřil na další konkrétní možnosti zpracování osobních údajů na pracovišti, jako je monitoring zaměstnanců pomocí služebních emailů, telefonů a GPS ve služebních automobilech. Na závěr této kapitoly jsem zveřejnil výsledky dotazníkového šetření, u kterého byl cíl obsáhnout co nejvíce zaměstnanců na rozdílných pracovních pozicích. Otázky jsem mířil jednak na četnost využití kamerového systému zaměstnavatelem, aby se mi potvrdil předpoklad, že většina zaměstnavatelů tento systém využívá. Poté jsem udělal průzkum o povinnosti informovat zaměstnance, kdy jsem na základě zjištění z odpovědí došel k závěru, že zaměstnavatel tuto informační povinnost o zpracování údajů zaměstnanců v drtivé většině dodržuje, neboť si uvědomuje možnost tvrdé sankce, při nerespektování této povinnosti. Poslední dvě otázky v dotazníkovém šetření byly mířeny na celkový dojem zaměstnanců z GDPR, kdy vyšlo najevo, že Nařízení z pohledu zaměstnanců je funkční, jeho roli vnímají a kvitují jeho prospěch. U každé otázky byla zmíněna prognóza a zhodnocení, kdy můžu konstatovat, že jsem příliš ve svých odhadech neodchyloval od výsledku.

Závěrečná část diplomové práce se zabývala judikaturou. Nejdříve jsem popsal úlohu dozorového úřadu, kterým je v České republice Úřad pro ochranu osobních údajů, jenž má za úkol sledovat dodržování Nařízení a sankcionovat případné porušení. Nařízení dále upravuje obsazení dozorového úřadu a možné odvolání jeho členů. Činnost Úřadu pro ochranu osobních údajů jsem reflektoval do třech případů kontroly, kterou ÚOOÚ v oblasti pracovního práva uskutečnil. Ve všech případech po jejich rozboru jsem upozoroval, že ÚOOÚ plní svoji funkci účelně.

Sedmou a poměrně obsáhlou kapitolu diplomové práce jsem věnoval judikatuře, neboť reflektování předpisu a výklad judikatury, může být pro další obdobné případy velmi důležité. Proto jsem vždy použil konkrétní důležitý pojem, který jsem dříve v diplomové práci zmiňoval a vyhledal příslušný judikát na danou problematiku. Vyhledal jsem rozhodnutí Soudního dvoru Evropské unie, Evropského soudu pro lidská práva a také rozhodnutí Nejvyššího správního soudu ČR.

Cílem diplomové práce bylo provést čtenáře od teoretické přes praktickou do judikaturní části tak, aby si dokázal u vybraných judikátů vytvořit pohled na konkrétní skutkovou podstatu a ze získaných poznatků z předchozích částí jí analyzovat v kontextu GDPR. Pokud se tomu tak stalo, dovoluji si konstatovat, že jsem cíl diplomové práce splnil.

Cizojazyčné resumé

The aim of the diploma thesis was to comprehensively explain to the reader the impact of the GDPR on labor law. In the opening chapter, I focused on the historical formation of personal data protection, which, even with the development of modern technologies and with it easier access to data, must continue to innovate and establish narrower barriers for their modification, processing and acquisition. Through such a process, the protection of personal data reached the General Regulation, which entered into force on May 24, 2018 and canceled the previous directive 95/46/EC, which in some aspects was no longer enough for the innovation of modern technologies, and since it was a directive, there was no obligation direct legal obligations for EU member states. Therefore, it was necessary to issue a uniform legal regulation that will directly oblige the EU member states to implement it. In order to understand the meaning of the GDPR, it was necessary to understand the individual concepts that make it up. Another chapter of the theoretical part of the diploma thesis was devoted to this, which gradually analyzed key terms in the sphere of personal data protection in its sub-chapters. Furthermore, I focused on the most important principles, which can be perceived as the guiding ideas in the spirit of which the Regulation is based and which cannot be deviated from, because then the very essence of the legal regulation would be violated.

The second, practical part, first offered the reader an analysis of the processing of personal data in the individual phases of the employment relationship and clarified to what extent the employer can process the employee's data according to the Regulation with reference to individual practical examples. I also mentioned the important aspect of the prohibition of discrimination before employment, because personal information such as gender or religion can be a potential obstacle for employers to hire an employee. I thus determined the situations in which the employer moves between and when beyond the boundaries of the law. A relatively large part was devoted to the employee's personal file, as I perceive it as the most intensive processing of personal data during the employment relationship. I have also listed other situations where it is possible to encounter the processing of personal data at the workplace, such as the attendance system or the question of salary data. Although it may seem that upon termination of employment, the employer should have nothing to do with the employee from the moment the last salary is paid and the employee's right to "be forgotten" under the Regulation applies, this statement is not entirely true. This is the focus of the analysis of the last phase of the employment relationship, i.e. after termination, the employer may retain the employee's personal data for cases specified by law, but certain processing is still ongoing.

In the fifth chapter, I devoted myself to practical examples of monitoring employees at the workplace, followed by a questionnaire survey, in which I asked 37 employees who work at different workplaces, questions related to monitoring. The camera system can be described as the most popular and most frequent monitoring of employees. This will make it clear to the reader under what conditions this system can be used. I also focused on other specific possibilities for processing personal data at the workplace, such as monitoring employees using work emails, phones and GPS in company cars. At the end of this chapter, I published the results of a questionnaire survey, the goal of which was to include as many employees as possible in different job positions. I aimed the questions at the frequency of use of the camera system by the employer in order to confirm the assumption that most employers use this system. I then conducted a survey on the obligation to inform employees, when, based on the findings from the answers, I came to the conclusion that the employer overwhelmingly complies with this obligation to inform about the processing of employee data, as it is aware of the

possibility of a severe penalty in case of non-respect of this obligation. The last two questions in the survey were aimed at the employees' overall impression of the GDPR, when it became clear that the Regulation is functional from the employees' point of view, they perceive its role and acknowledge its benefit. For each question, a forecast and an evaluation were mentioned, where I can state that I did not deviate too much from the result in my estimations.

The final part of the thesis dealt with jurisprudence. First, I described the role of the supervisory authority, which in the Czech Republic is the Office for the Protection of Personal Data, which has the task of monitoring compliance with the Regulation and sanctioning any violations. The regulation also regulates the staffing of the supervisory authority and the possible dismissal of its members. I reflected the activities of the Office for the Protection of Personal Data in three cases of control carried out by the ÚOOÚ in the field of labor law. In all cases, after their analysis, I observed that the ÚOOÚ fulfills its function effectively.

I dedicated the seventh and relatively comprehensive chapter of the diploma thesis to jurisprudence, because reflecting on the regulation and interpretation of jurisprudence can be very important for other similar cases. That's why I always used a specific important concept that I mentioned earlier in my diploma thesis and searched for relevant case law on the given issue. I looked up the decisions of the Court of Justice of the European Union, the European Court of Human Rights and also the decisions of the Supreme Administrative Court of the Czech Republic.

The aim of the diploma thesis was to guide the reader from the theoretical to the practical to the jurisprudential part so that he could create a view of the specific facts of the selected jurisprudence and analyze it in the context of the GDPR based on the knowledge gained from the previous parts. If that is the case, I can state that I have fulfilled the aim of the diploma thesis.

Seznam použité literatury

Knižní publikace

- MORÁVEK, J. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, 2019. ISBN 978-80-7598-588-0
- ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3.
- NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. **GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář**. 2. vydání. Praha: Wolters Kluwer ČR, 2018. ISBN 978-80-7598-069-4
- BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5.,
- NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7

Internetové zdroje

- Kontrola zveřejňování fotografií zaměstnanců na internetových stránkách zaměstnavatele (UOOU-03225/19). *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/kontrola-zverejnovani-fotografii-zamestnancu-na-internetovych-strankach-zamestnavatele-uoou-03225-19/ds-6474/archiv=0&p1=6243>
- Kontrola zpracování osobních údajů bývalých zaměstnanců (společnost Randstad s.r.o.). *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-byvalych-zamestnancu-spolecnost-randstad-s-r-o/ds-5709/archiv=0&p1=5649>
- Kontrola zpracování osobních údajů bývalých zaměstnanců (společnost 42 Financial Services a.s.). *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-byvalych-zamestnancu-spolecnost-42-financial-services-a-s/ds-5731/archiv=0&p1=5653>
- Albánská prokuratura vyšetřuje únik osobních údajů 700.000 lidí, včetně premiéra. *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/albanska-prokuratura-vysetruje-unik-osobnich-udaju-700-000-lidi-vcetne-premiera/ds-6914/archiv=0&p1=3938>

- Barbulescu proti Rumunsku. *Eslp.justice.cz* [online]. Dostupné z: http://eslp.justice.cz/justice/judikatura_eslp.nsf/WebSearch/4C37F9ACAF53B7AC125822E004D8EFF?openDocument&Highlight=0
- IKEA špehovala zaměstnance, rozhodl francouzský soud. Má zaplatit milion eur. *Uoou.cz* [online]. Dostupné z: https://www.idnes.cz/ekonomika/zahranicni/ikea-soud-francie-pokuta-spehovani.A210615_112940_eko-zahranicni_mato
- Copland proti Velké Británii. *Ictjudikatura.law.muni.cz* [online]. Dostupné z: https://ictjudikatura.law.muni.cz/wiki/62617/00_-
- Řetězec H&M zavře 250 obchodů. Navíc dostal obří pokutu za špehování zaměstnanců. *Uoou.cz* [online]. Dostupné z: <https://www.uoou.cz/retezec-h-amp-m-zavre-250-obchodu-navic-dostal-obri-pokutu-za-spehovani-zamestnancu/ds-6377/archiv=0&p1=3938>

Právní předpisy

- Všeobecná deklarace lidských práv schválená Organizací spojených národů dne 10.12.1948
- Mezinárodní pakt o občanských a politických právech a Mezinárodní pakt o hospodářských, sociálních a kulturních právech, publikované jako vyhláška ministra zahraničních věcí č. 120/1976 Sb.
- Úmluva o ochraně dat se zřetelem na automatizované zpracování osobních dat ze dne 28. 1. 1981
- Dodatkový protokol k Úmluvě o ochraně osob
- Zákon č. 273/2008 Sb., Zákon o Policii ČR
- Nařízení EU č. 2016/679, Obecné nařízení o ochraně osobních údajů
- Zákon 262/2006 Sb., Zákoník práce
- Zákon č. 361/2003 Sb., zákon o služebním poměru příslušníků bezpečnostních sborů
- Zákon č. 234/2014 Sb., Zákon o státní službě
- Zákon č. 582/1991 Sb., zákon o organizaci a provádění sociálního zabezpečení
- Zákon č. 187/2006 Sb., o nemocenském pojištění
- Zákon č. 186/2016 Sb., zákon o hazardních hrách

- Zákon č. 307/2013 Sb., zákon o povinném značení lihu
- Zákon č. 316/2014 Sb., zákon o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti
- Listina základních práv a svobod
- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 110/2019 Sb., zákon o zpracování údajů
- Zákon č. 500/2004 Sb., správní řád

Judikatura

Kontrola prováděná ÚOOÚ:

- Kontrola zveřejňování fotografií zaměstnanců na internetových stránkách zaměstnavatele (ÚOOÚ-03225/2019)
- Kontrola zpracování osobních údajů bývalých zaměstnanců (společnost Randstad s.r.o.)
- Kontrola zpracování osobních údajů bývalých zaměstnanců (společnost 42 Financial Services a.s.)

Rozsudky Soudního dvora Evropské unie

- Rozsudek Soudního dvora ze dne 10. 7. 2018, *Jehovan todistajat*, C - 25/17,
- Rozsudek Soudního dvora ze dne 6. 11. 2003, *Lindquist*, C-101/01,
- Rozsudek Soudního dvora ze dne 11. 12. 2014, *Ryneš*, C-212/13
- Rozsudek Soudního dvora ze dne 13. 5. 2014, *Google Spain a Google*, C-131/12
- Rozsudek Soudního dvora, *Schwartz*, C-291/12

Rozsudky českých soudů:

- Nejvyšší správní soud České republiky sp. zn. 1 As 13/2011-210
- Nejvyšší soud České republiky sp. zn. 21 Cdo 2305/2015
- Nejvyšší soud České republiky sp. zn. 21 Cdo 4429/2013

- Rozsudky Evropského soudu pro lidská práva:
- López Ribalda proti Španělsku (č. 1874/13)
- Barbulescu proti Rumunsku (č. 61496/08)
- Copland proti Velké Británii (62617/00)

Rozsudky jiných vnitrostátních soudů:

- Esch-Leonhardt a další v. ECB, T-320/02
- Nikolaou v. Komise