UNIVERZITA KARLOVA

Právnická fakulta

Eliška Trinerová

Práva a povinnosti zaměstnavatele jako správce osobních údajů

Diplomová práce

Vedoucí diplomové práce: JUDr. Jakub Morávek, Ph.D.

Katedra pracovního práva a práva sociálního zabezpečení

Datum vypracování práce (uzavření rukopisu): 8. 4. 2019

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

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 293612 znaků včetně mezer.

_____

Eliška Trinerová

V Praze dne 8. 4. 2019

Poděkování

Děkuji JUDr. Jakubu Morávkovi, Ph.D., vedoucímu diplomové práce, za ochotu vést moji diplomovou práci a za cennou pomoc a připomínky při jejím vypracování. Zároveň též děkuji svojí rodině za podporu během celého studia.

Obsah

Úvod

Ochrana osobních údajů je oblastí, která stále více získává, nebo by minimálně měla získávat pozornost nejen odborníků, ale též široké veřejnosti. Svůj podíl na stále větší aktuálnosti tohoto tématu má jistě neustávající rozvoj v oblasti technologií (zejména informačních technologií), který s sebou nese provádění zpracování osobních údajů v obrovském rozsahu.

Nemalou roli v tom, že se ochrana osobních údajů stává stále více diskutovaných témat, nyní hraje i skutečnost, že dne 25. 5. 2018 nabylo účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) („GDPR“), tedy poměrně dlouho očekávaný a diskutovaný právní předpis, který by měl dopomoci k nastavení jednotného rámce ochrany osobních údajů na celém území EU. GDPR v mnohých lidech, i téměř rok po jeho účinnosti, vzbuzuje dojem, že se jedná o revoluci v ochraně osobních údajů, která znamená značné navýšení povinností správců ve vztahu k jimi prováděnému zpracování osobních údajů.

GDPR z pohledu českých správců osobních údajů, jimiž jsou typicky i zaměstnavatelé, jistě přineslo několik nových povinností a institutů, nebo alespoň blíže rozvedlo ty stávající, rozhodně ale, dle názoru autorky, není třeba propadat panice a pocitu, že jen kvůli účinnosti GDPR bude třeba vynakládat enormní administrativní a finanční prostředky na dosažení souladu všech interních procesů správců s pravidly na ochranu osobních údajů.

Hlavním cílem této diplomové práce není poskytnout přehled všech povinností, které se vztahují na správce osobních údajů, jelikož by, s přihlédnutím k obsáhlosti tohoto tématu, nebylo možné toto téma v celé šíři postihnout, ale blíže analyzovat některé z povinností, se kterými se mnozí správci musí po účinnosti GDPR nově vypořádat. S ohledem na jejich význam zároveň autorka považovala za důležité v této práci analyzovat zcela základní povinnosti správců osobních údajů, které úzce souvisí se základními zásadami zpracování osobních údajů. Zároveň je v práci uceleně blíže nastíněn mj. vývoj ochrany osobních údajů s důrazem na GDPR, včetně zdůraznění hlavních změn, které tento předpis přinesl, stejně jako základní pojmy, se kterými GDPR operuje. Autorka se v některých pasážích bude věnovat též srovnání právní

úpravy konkrétních institutů před a po účinnosti GDPR, byť komparace není hlavním cílem této práce, a dále se též pokusí o poskytnutí kritického náhledu na některé z povinností, které správcům ukládá GDPR.

Při analýze a hodnocení jednotlivých institutů ochrany osobních údajů je pozornost věnována též relevantním případům zpracování osobních údajů zaměstnavatelem v pracovněprávních vztazích.

Tato diplomová práce je rozdělena do čtyř kapitol. V první kapitole je obsažen krátký historický exkurz do úpravy ochrany osobních údajů, který shrnuje zejména hlavní dokumenty obsahující úpravu ochrany osobních údajů, a to jak na národní, tak na unijní a mezinárodní úrovni. Podstatná část první kapitoly je věnována GDPR a shrnutí hlavních důvodů pro jeho přijetí či hlavních změn, které přineslo, nebo vlivu přijetí GDPR na národní právní úpravu.

Druhá kapitola je věnována systematickému vymezení základních pojmů, se kterými operuje GDPR. Třetí kapitola pak obsahuje souhrn základních zásad zpracování osobních údajů, které představují základní povinnosti správce, jimiž se musí řídit při zpracování osobních údajů. Do této kapitoly je zařazen i přehled a rozbor právních důvodů pro zpracování osobních údajů, které jsou taxativně vyčteny v GDPR.

V poslední kapitole jsou pak blíže rozebrány vybrané povinnosti správce osobních údajů, konkrétně pak některé z povinností, které lze v českém prostředí v zásadě označit za nové – povinnost vést záznamy o činnostech zpracování, povinnost provádět posouzení vlivu na ochranu osobních údajů a povinnost jmenovat pověřence pro ochranu osobních údajů, tedy povinnosti, které se sice nutně nevztahují na všechny správce, nicméně i s ohledem na určité nejasnosti při interpretaci skutečnosti, na koho se tyto povinnosti vztahují, mohou být pro mnoho správců aktuální.

1 Přehled právní úpravy ochrany osobních údajů

První kapitola zahrnuje stručný přehled vývoje ochrany osobních údajů na úrovni mezinárodní, unijní i národní, včetně vymezení nejdůležitějších dokumentů upravujících tuto oblast. Důraz bude kladen zejména na zcela nejnovější právní úpravu ochrany osobních údajů, tedy na Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) („GDPR"), včetně nastínění důsledků účinnosti GDPR pro národní právní úpravu ochrany osobních údajů.

1.1 Právní úprava ochrany osobních údajů na mezinárodní úrovni

Prvními dokumenty, které mají význam pro vývoj ochrany osobních údajů, jsou ty dokumenty upravující obecně základní lidská práva a svobody, zejména pak právo na soukromí. Ochranou soukromí se ve světě zřejmě poprvé zabývala Deklarace práv člověka a občana přijata ve Francii v roce 1789.[1] Za první opravdu celosvětově významný mezinárodní dokument garantující právo na soukromí lze považovat Všeobecnou deklaraci lidských práv, která byla přijata Valným shromážděním Organizace spojených národů v San Franciscu v roce 1948.[2] Z hlediska ochrany soukromí je významný zejména čl. 12 Všeobecné deklarace lidských práv, který stanoví, že *„nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům."* Všeobecná deklarace lidských práv sice nikdy nebyla právně závazná, nicméně i tak nelze snižovat její význam pro mezinárodní úpravu práva na soukromí. Znění čl. 12 Všeobecné deklarace lidských práv navíc bylo doslovně přejato do čl. 17 Mezinárodního paktu o občanských a politických právech přijatého rovněž Organizací spojených národů v roce 1966.[3] Tento dokument již má povahu právně závazné mezinárodní smlouvy a je jím vázaná i Česká republika.

1 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 27, ISBN 978-80-7380-689-7.
2 ŽŮREK, J. *Praktický průvodce GDPR*, Praha: ANAG, 2017, s. 13, ISBN 978-80-7554-097-3.
3 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*, op. cit. s. 27.

Právo na soukromí je zakotveno též v další, z hlediska ochrany základních práv a svobod, velmi významné mezinárodní smlouvě, a to v Úmluvě o ochraně lidských práv a základních svobod přijaté na půdě Rady Evropy v roce 1950 („Evropská úmluva“). Evropská úmluva v čl. 8 deklaruje právo na respektování rodinného a soukromého života, v čl. 10 ale zároveň stanovuje svobodu projevu, tedy právo, které je v protikladu s právem obsaženým v čl. 8. Obě tato práva jsou nicméně bez veškerých pochybností zcela zásadní pro fungování moderní demokratické společnosti.[4]

První komplexní dokument, který se zabývá již přímo ochranou osobních údajů, byl přijat až o několik desítek let později. Jedná se o Úmluvu Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat přijatou dne 28. ledna 1981 ve Štrasburku. Tato Úmluva je známá jako Úmluva č. 108.[5] Účelem Úmluvy č. 108, jak plyne z jejího čl. 1, je garance úcty k právům a základním svobodám fyzické osoby, zejména pak k právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů. Úmluva č. 108 obsahuje mj. definici pojmu osobní údaj, která se v zásadě nijak významně neliší od dnešního pojetí definice tohoto pojmu[6], dále přehled základních zásad pro ochranu údajů[7] a věnuje se též přeshraničnímu přenosu osobních údajů.[8] Jak napovídá samotný název Úmluvy č. 108, do její působnosti má náležet pouze automatizované zpracování dat a automatizované soubory osobních údajů.

Česká republika Úmluvu č. 108 ratifikovala až v roce 2000, tedy v roce, kdy byl přijat zákon č. 101/2000 Sb., o ochraně osobních údajů („ZOOÚ“). Teprve ZOOÚ byl totiž, na rozdíl od dříve platného a účinného zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, plně v souladu s Úmluvou č. 108.[9]

4 MAŠTALKA, J. *Osobní údaje, právo a my. 1. vydání*. Praha: C. H. Beck, 2008, s. 5, ISBN 978-80-7400-033-1.

5 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*., op. cit. s. 27.

6 Srov. čl. 2 písm. a) Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. 1. 1981.

7 Srov. hlava II Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. 1. 1981.

8 Srov. hlava III Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. 1. 1981.

9 MAŠTALKA, J. *Osobní údaje, právo a my. 1. vydání*., op. cit. s. 11-12.

1.2 Právní úprava ochrany osobních údajů na unijní úrovni

1.2.1 Vývoj právní úpravy před účinností GDPR

Východisko pro oblast ochrany osobních údajů na úrovni práva Evropské unie (EU) je možné nalézt v primárním právu. Konkrétně je nutné poukázat na čl. 16 Smlouvy o fungování EU, který v odst. 1 zakotvuje právo každého jedince na ochranu osobních údajů, v odst. 2 pak předvídá přijetí závazných pravidel o ochraně fyzických osob při zpracování osobních údajů a o volném pohybu těchto údajů Evropským parlamentem a Radou EU. Čl. 16 odst. 2 Smlouvy o fungování EU se stal oporou pro přijetí Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů („Směrnice 95/46/ES“), stejně jako pro přijetí GDPR.

V oblasti primárního práva EU je z hlediska významu pro právo na ochranu osobních údajů třeba zmínit i Listinu základních práv EU. Ta garantuje právo na ochranu osobních údajů v čl. 8 odst. 1. Čl. 8 odst. 2 Listiny základních práv EU pak zní následovně *„Tyto (osobní) údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.“* Zakotvuje tedy některé elementární zásady zpracování osobních údajů a práva subjektů údajů. V odst. 3 stejného článku je pak uvedeno, že dodržování pravidel týkajících se ochrany osobních údajů má kontrolovat nezávislý orgán.

Nejdůležitějším dokumentem v oblasti ochrany osobních údajů v rámci sekundárního práva EU i v rámci práva EU obecně byla před účinností GDPR beze sporu Směrnice 95/46/ES. Směrnice 95/46/ES se v mnohém inspirovala Úmluvou č. 108. Oproti Úmluvě č. 108 však pojala zpracování osobních údajů komplexněji, když se vztahovala nejen na automatizované zpracování osobních údajů, ale také na zpracování neautomatizované za předpokladu, že jsou neautomatizovaně zpracovány osobní údaje, které jsou nebo mají být obsaženy v rejstříku ve smyslu čl. 2 písm. c) Směrnice 95/46/ES.[10] Směrnice sestávala z 34 článků, kterým předcházelo 72 recitálů. Tyto recitály měly zejména osvětlit cíle, účel Směrnice 95/46/ES a obecné zásady, čímž

10 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 14-15.

poskytovaly vodítko pro interpretaci samotných článků Směrnice 95/46/ES.[11] Hlavním cílem Směrnice 95/46/ES bylo stanovení jednotné úpravy ochrany osobních údajů v evropském prostoru a odstranění překážek toku osobních údajů na území Evropského společenství.[12]

Směrnice 95/46/ES vymezuje základní pojmy související s ochranou osobních údajů, a to v daleko širší míře oproti Úmluvě č. 108, dále specifikuje zásady pro zpracování osobních údajů, obsahuje také výčet práv a povinností subjektů údajů a správce nebo pravidla pro předávání osobních údajů do třetích zemí.

V čl. 28 Směrnice 95/46/ES stanovila členským státům též povinnost pověřit určitý orgán veřejné moci dohledem nad dodržování pravidel na ochranu osobních údajů stanovených touto Směrnicí, resp. právními předpisy, které členské státy přijaly na základě Směrnice. V České republice se tímto orgánem stal Úřad pro ochranu osobních údajů, který byl zároveň ZOOÚ zřízen.[13]

Významným ustanovením ve Směrnici 95/46/ES je rovněž čl. 29, kterým byla zřízena pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů (WP29). Hlavním úkolem tohoto nezávislého poradního orgánu bylo zejména posuzování otázek souvisejících s uplatňováním vnitrostátních předpisů provádějících Směrnici 95/46/ES, přijímání stanovisek pro Evropskou komisi pojednávajících o úrovni ochrany osobních údajů v EU a poskytování poradenství Evropské komisi ohledně případných návrzích změn této Směrnice.[14]

Jelikož směrnice nestanovuje přímo práva a povinnosti subjektům práva členských států, ale pouze cíl, který musí všechny členské státy EU splnit, byly státy EU povinny implementovat Směrnici 95/46/ES do svých právních řádů. K tomu jim byla stanovena lhůta tří let od přijetí Směrnice 95/46/ES, s tím, že v této lhůtě musel daný vnitrostátní právní předpis nabýt účinnosti.[15] Do českého právního řádu byla Směrnice 95/46/ES transponována skrze ZOOÚ.

Směrnici 95/46/ES se do určité míry zdařilo sjednotit právní úpravu ochrany osobních údajů v evropském měřítku, avšak jednotlivé členské státy EU netransponovaly směrnici identicky, a dílčí právní úpravy ochrany osobních údajů přijaté na úrovni členských států se od sebe v mnohém lišily. K úplné harmonizaci

11 MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích. 1. vydání.* Praha: Wolters Kluwer, 2013, s. 121, ISBN 978-80-7478-139-1.
12 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*, op. cit. s. 27.
13 Srov. § 2 ZOOÚ.
14 Srov. čl. 30 Směrnice 95/46/ES.
15 Čl. 32 odst. 1 Směrnice 95/46/ES.

právní úpravy ochrany osobních údajů v rámci EU tedy nedošlo. Jako příklad odlišné úpravy napříč Evropskou unií lze uvést institut pověřence pro ochranu osobních údajů, který byl v některých státech zakotven povinně, v jiných fakultativně a v dalších nebyl tento institut právně upraven vůbec. Dále např. v Nizozemí byla upravena, nad rámec povinností vyplývajících ze Směrnice 95/46/ES, ohlašovací povinnost pro případy porušení zabezpečení ochrany osobních údajů.[16] Na roztříštěnost při provádění ochrany osobních údajů v rámci EU a rozdíly v úrovni práva na ochranu osobních údajů fyzických osob napříč členskými státy EU způsobené odlišným prováděním a uplatňováním Směrnice 95/46/ES ostatně poukazuje i recitál 9 GDPR.

1.2.2 GDPR

V průběhu více než dvaceti let, které uplynuly od účinnosti Směrnice 95/46/ES, docházelo k rychlému vývoji nových technologií, příkladem je rozvoj internetových nabídek a služeb, rozvoj elektronického obchodování, stále rozšířenější využívání různých sociálních sítí, s čímž samozřejmě souvisí též rozsáhlejší sbírání a zpracování osobních údajů, včetně monitorování a profilování jedinců.

EU se proto, s cílem přizpůsobit právní úpravu ochrany osobních údajů výše popsanému vývoji, rozhodla učinit reformu právního rámce pro ochranu osobních údajů a dne 27. dubna 2016 vstoupilo v platnost GDPR, které nabylo účinnosti 25. května 2018 a nahradilo Směrnici 95/46/ES. Dvouletou legisvakanční lhůtu lze považovat za poměrně dlouhou, její stanovení však nebylo bezdůvodné. Právě ve lhůtě dvou let od platnosti GDPR totiž všichni ti, kdo zpracovávají osobní údaje, měli zajistit uvedení zpracování osobních údajů do souladu s GDPR.[17]

Dalším z hlavních cílů GDPR je také *zajistit soudržnou a vysokou úroveň ochrany fyzických osob a odstranit překážky bránící pohybu osobních údajů v rámci Unie*[18]. Úroveň ochrany osobních údajů by přitom měla být ve všech členských státech EU rovnocenná a pravidla související s ochranou fyzických osob při zpracování osobních údajů by měla být uplatňována jednotně.[19] Aby byla tato rovnocenná úroveň ochrany osobních údajů napříč všemi členskými státy EU co nejlépe zajištěna, byla pro nový nástroj ochrany osobních údajů zvolena právě forma nařízení. Nařízení, jakožto právní akt přímo aplikovatelný v každém členském státu EU, má větší sjednocující efekt

16 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 15.
17 Recitál 171 GDPR.
18 Recitál 10 GDPR.
19 Tamtéž.

než směrnice. Na rozdíl od směrnice se tedy pravidla stanovená v nařízení přímo vztahují na vnitrostátní subjekty a nevyžaduje se, aby došlo k jeho transpozici do právního řádu členského státu. To ovšem neznamená, že by členské státy v souvislosti s účinností GDPR neměly v rámci svého vnitrostátního právního řádu činit žádné kroky.

Členské státy musí v souladu s GDPR přizpůsobit své vnitrostátní právní předpisy tomuto nařízení, a to přijetím nových právních předpisů či změnou stávajících právních předpisů.[20] Typicky budou na úrovni členských států přijímány tzv. adaptační zákony, které připraví právní řád členského státu na účinnost GDPR, a odstraní případný nesoulad národních právních norem s GDPR.[21]

Při přizpůsobování vnitrostátních předpisů GDPR přitom členské státy musí mít na paměti fakt, že pokud by jimi přijatá vnitrostátní opatření způsobila vytvoření překážky pro přímou použitelnost GDPR a ohrožení současného a jednotného uplatňování GDPR v rámci celé EU, budou tato v rozporu se smlouvami.[22] Členské státy by dále měly respektovat zákaz opakování znění GDPR ve vnitrostátních právních předpisech, není-li to nutné za účelem soudržnosti a učinění vnitrostátních právních předpisů srozumitelnými pro jejich adresáty.[23]

GDPR v některých případech stanoví konkrétní povinnost členských států upravit určité aspekty ve vnitrostátním právním předpise. Všechny členské státy tak musí právním předpisem upravit záležitosti související se zřízením vnitrostátních úřadů pro ochranu osobních údajů (zejména samotné zřízení dozorového úřadu, pravidla jmenování členů dozorového úřadu, podmínky pro jmenování členů dozorového úřadu a délka jejich funkčního období)[24]. Členské státy jsou dále povinny učinit volbu akreditačního orgánu pro subjekty vydávající osvědčení o ochraně osobních údajů[25] a zajistit uvedení práva na ochranu osobních údajů dle GDPR do souladu s právem na svobodu projevu a informací.[26]

GDPR také v určitých záležitostech dává členským státům možnost tyto upravit či upřesnit na vnitrostátní úrovni, přičemž záleží jen na vůli zákonodárců daných

20 Sdělení Komise Evropskému parlamentu a Radě ze dne 16. 8. 2018, COM(2018) 43 final/2, dostupné na http://ec.europa.eu/transparency/regdoc/rep/1/2018/CS/COM-2018-43-F2-CS-MAIN-PART-1.PDF.

21 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 19.

22 Rozsudek Soudního dvora ve věci 94/77, *Fratelli Zerbone Snc v. Amministrazione delle finanze dello Stato*, ECLI:EU:C:1978:17 a 101.

23 Sdělení Komise Evropskému parlamentu a Radě ze dne 16. 8. 2018, COM(2018) 43 final/2, op. cit. a recitál 8 GDPR.

24 Čl. 54 odst. 1 GDPR.

25 Čl. 43 odst. 1 GDPR.

26 Čl. 85 odst. 1 GDPR.

členských států, zda takovou možnost využijí, či nikoliv. Poskytnutí prostoru pro upřesnění či stanovení vlastních pravidel v některých aspektech zpracování osobních údajů je nastíněno již v recitálu 10 GDPR.[27] Níže je uveden demonstrativní výčet případů, kdy členské státy fakultativně mohou určité aspekty upravit na vnitrostátní úrovni.

GDPR např. umožňuje členským státům blíže určit požadavky na zpracování osobních údajů k zajištění jeho zákonnosti a spravedlivosti, pokud jde o zpracování za účelem plnění právní povinnosti správce, nebo za účelem plnění úkolu ve veřejném zájmu či při výkonu veřejné moci.[28] GDPR též dává členským státům prostor odchýlit se od věkové hranice stanovené pro souhlas dítěte v souvislosti se službami informační společnosti s tím, že dodrží podmínku, aby taková věková hranice nebyla nižší než 13 let.[29] Členské státy jsou dále oprávněny stanovit vlastní pravidla ohledně zpracování genetických a biometrických údajů a údajů o zdravotním stavu.[30] Prostor pro vnitrostátní právní úpravu je členským státům dán i ohledně možného oprávnění neziskových a dalších subjektů vyčtených v čl. 80 odst. 1 GDPR podat stížnost u dozorového úřadu a vykonávat práva dle čl. 78 a 79 GDPR i bez pověření od subjektu údajů v případě domněnky, že došlo k porušení práv subjektu údajů při zpracování jeho osobních údajů.[31]

Z hlediska zpracování osobních údajů v rámci pracovněprávních vztahů je důležité poukázat na článek 88 GDPR, který zmocňuje členské státy, aby stanovily *konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména za účelem náboru, plnění pracovní smlouvy včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a rozmanitosti na pracovišti, zdraví a bezpečnosti na pracovišti, ochrany majetku zaměstnavatele nebo majetku zákazníka, dále za účelem individuálního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru.* Tento článek ve spojení s článkem 9 odst. 2 písm.

27 V recitálu 10 GDPR je mj. uvedeno, že členské státy mají mít možnost na vnitrostátní úrovni konkretizovat aplikaci pravidel GDPR, pokud se jedná o zpracování osobních údajů z titulu plnění právnich povinností či provádění úkolu ve veřejném zájmu nebo při výkonu veřejné moci a že v členských státech *existuje několik právních předpisů specifických pro určitá odvětví v oblastech, ve kterých je třeba přijmout konkrétnější ustanovení.* Dále je zde deklarován určitý prostor pro stanovení vlastních pravidel pro zpracování zvláštních kategorií osobních údajů.

28 Čl. 6 odst. 2 GDPR.

29 Čl. 8 odst. 1 GDPR.

30 Čl. 9 odst. 4 GDPR.

31 Čl. 80 odst. 2 GDPR.

b) GDPR tedy umožňuje členským státům konkretizovat pravidla o ochraně osobních údajů zaměstnanců. Pokud členské státy na základě čl. 88 GDPR stanoví určitá pravidla, platí, že tato musí zahrnovat *zvláštní a vhodná opatření zajišťující ochranu lidské důstojnosti, oprávněných zájmů a základních práv subjektů údajů*.[32] V souladu s čl. 88 odst. 3 GDPR musí členské státy splnit notifikační povinnost vůči Komisi, pokud přijmou či změní právní předpis dle odst. 1 téhož článku.

Z výše uvedeného plyne, že i ve věci ochrany osobních údajů zaměstnanců bude nutné se řídit ustanoveními GDPR, avšak přijme-li členský stát speciální právní úpravu v souladu s čl. 88 GDPR, bude tento vnitrostátní právní předpis předpisem speciálním vůči GDPR jakožto předpisu obecnému, a při aplikaci právní úpravy se bude postupovat v souladu se zásadou lex specialis derogat legi generali.[33]

Přestože nelze GDPR upřít, že, oproti Směrnici 95/46/ES, má již svoji povahou větší potenciál zamezit zásadním rozdílům v úrovni ochrany osobních údajů v jednotlivých členských státech EU, a naplnit tak cíle stanovené v recitálu 13,[34] existuje několik opodstatněných argumentů, že ani přijetí GDPR nemusí znamenat, že dojde k naplnění cíle jednotné aplikace. Prvním argumentem je skutečnost, že na národní úrovni budou aplikaci právní úpravy sjednocovat orgány, které budou oprávněny k přezkumu rozhodnutí národních úřadů pro ochranu osobních údajů (typicky správní soudy); nelze tedy vyloučit, že v různých státech nedojde při sjednocování aplikace právní úpravy k odchylkám. Další argument vychází z výše zmíněného přijímání národních právních předpisů, které přizpůsobují národní právní řád na účinnost GDPR, nebo konkretizují či stanovují pravidla tam, kde to GDPR vyžaduje nebo umožňuje. Opět platí, že různé členské státy mohou k dané věci přistoupit odlišně.[35]

Co se týče znění GDPR, nejdříve je vhodné se zaměřit na jeho strukturu. GDPR disponuje velmi obsáhlou preambulí tvořenou 173 tzv. recitály. Jedná se o číslované odstavce, které lze označit jako výkladovou pomůcku pro vlastní text GDPR. Dá se říci, že plní obdobnou funkci jako důvodová zpráva k zákonu. Preambule obsahuje mj.

32 Čl. 88 odst. 2 GDPR.

33 ZEMANOVÁ ŠIMONOVÁ, H. *Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů*. Bulletin advokacie 9/2017, s. 25.

34 Recitál 13 mj. stanoví, že cílem GDPR je zajistit, že ve všech členských státech budou mít subjekty údajů možnost domáhat se stejných práv souvisejících se zpracováním jejich osobních údajů, správcům a zpracovatelům budou stanoveny totožné základní povinnosti při jimi prováděném zpracování osobních údajů a ve všech členských státech budou též zakotveny rovnocenné sankce pro případ porušení pravidel pro zpracování osobních údajů. Odstranění rozdílů v úrovni ochrany osobních údajů napříč EU znamená odstranění překážek, které brání volnému pohybu osobních údajů v rámci vnitřního trhu.

35 MORÁVEK, J. *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy 13-14/2018, s. 487.

důvody a cíle přijetí GDPR jako celku i některých konkrétních institutů, které nově přináší, či instrukce, jak tyto chápat. Proto je pro úspěšnou práci s GDPR nutné znát nejen jeho vlastní text (zvláštní část), ale též preambuli, a vždy propojovat jednotlivé recitály s příslušnými články zvláštní části.[36] Vlastní text GDPR je pak rozčleněn do 11 kapitol a 99 článků. Ve srovnání se Směrnicí 95/46/ES je tedy GDPR výrazně obsáhlejší.

K samotnému obsahu je níže uvedeno jen několik základních bodů a srovnání hlavních rozdílů oproti Směrnici 95/46/ES, vybrané pasáže GDPR pak budou detailněji rozebrány v dalších kapitolách této diplomové práce.

Stejně jako Směrnice 95/46/ES, tak i GDPR se z pohledu věcné působnosti vztahuje v zásadě na zpracování osobních údajů automatizované (zcela či částečně) i neautomatizované (pokud jde o osobní údaje, které jsou nebo mají být obsažené v evidenci ve smyslu čl. 4 odst. 6 GDPR).[37] Z hlediska místního do působnosti GDPR patří zpracování osobních údajů související s činností provozovny správce či zpracovatele v EU, a to bez ohledu na to, jestli zpracování probíhá přímo v EU, nebo nikoliv[38]. V čl. 3 odst. 2 jsou pak uvedeny případy, kdy se GDPR vztahuje na zpracování osobních údajů navzdory tomu, že správce nebo zpracovatel není usazen v EU. Úprava definic základních pojmů i zásad zpracování osobních údajů je v podstatě převzata ze Směrnice 95/46/ES s tím, že v některých aspektech došlo k jejímu rozšíření či modifikaci (např. nově uvedené definice pojmů genetické a biometrické údaje, pseudonymizace).[39]

V GDPR se objevuje nové pojetí principu odpovědnosti správce a přístup založený na riziku. Princip odpovědnosti správce není úplnou novinkou, ve Směrnici 95/46/ES byla odpovědnost správce zakotvena v čl. 23. GDPR ale princip odpovědnosti správce rozvíjí, když kromě výslovného stanovení odpovědnosti správce za splnění povinností uvedených v GDPR, ukládá správci povinnost soulad s GDPR doložit. Konkrétně lze odkázat na čl. 24 odst. 1 GDPR, dle kterého platí, že správce je povinen zavést vhodná technická a organizační opatření, aby mohl zajistit a doložit, že je zpracování osobních údajů prováděno v souladu s GDPR. Zavedená opatření správce musí, dle potřeby, revidovat a aktualizovat. Odpovědnost za dodržení povinností a povinnost být schopen toto doložit, je výslovně zakotvena též u zásad zpracování

36 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*, op. cit. s. 30.
37 Čl. 2 odst. 1 GDPR.
38 Čl. 3 odst. 1 GDPR.
39 MAŠTALKA, J. *Nové nařízení EU o ochraně osobních údajů a některé záležitosti spojené s jeho aplikací v ČR*. Právní rozhledy 21/2016.

osobních údajů v čl. 5 odst. 2 GDPR. GDPR obsahuje také nové standardizované nástroje, prostřednictvím kterých bude správce moci prokazovat soulad zpracování. Jedná se zejména o záznamy o činnostech zpracování, kodexy chování, možnost získání osvědčení nebo pověřenec pro ochranu osobních údajů. Soulad bude správce dále dokládat též řádným naplňováním práv subjektů údajů či spoluprací s dozorovým úřadem. Bude se vždy jednat o komplex činností, ne o jednu osamocenou činnost. Dosažení souladu zpracování osobních údajů s GDPR může pomoci i uplatňování principu *data protection by design*, tedy nastolení odpovídající ochrany osobních údajů už od návrhu činnosti, která znamená zpracování osobních údajů.[40]

Posun v pojetí principu odpovědnosti správce, který přineslo GDPR, někteří považují za důsledek regulatorního trendu, který je srovnatelný s vývojem institutu spotřebitele jakožto slabší smluvní strany. Vzhledem k tomu, že z různých průzkumů plyne omezená míra povědomí a schopnosti jednotlivců účinně se bránit proti porušování pravidel na ochranu osobních údajů, je nezbytné přesunout těžiště úpravy na povinné subjekty, aby byla zaručena účinnější ochrana práv subjektů údajů.[41]

Přístup založený na riziku obecně značí *povinnost správce a zpracovatele s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování a možným rizikům přijmout adekvátní technická a organizační opatření za účelem zajištění zabezpečení osobních údajů odpovídající riziku, které dané zpracování pro subjekty údajů představuje*. Takový přístup je smysluplný, protože různé zpracování je pro subjekty různě rizikové, a není možné určit shodnou hranici zabezpečení pro všechny správce. Takové pojetí principu založeného na riziku v podstatě znala i Směrnice 95/46/ES a ZOOÚ.[42] GDPR tento princip rozšiřuje a v jeho pojetí přístup založený na riziku znamená i aplikaci některých dodatečných povinností pro správce, a to v případech, kdy zpracování osobních údajů představuje riziko nebo vysoké riziko pro subjekty údajů. Platí princip, že čím vyšší riziko hrozí subjektům údajů, tím více povinností správce má. Tyto nové povinnosti se tak nevztahují plošně na všechny správce a zpracovatele a patří mezi ně povinnost vést záznamy o činnostech zpracování, povinnost jmenovat pověřence pro ochranu osobních údajů, provádět posouzení vlivu na ochranu osobních údajů, povinnost předchozí konzultace

40 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 26.

41 KISS, A., SZÖKE, G. L. *Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation* in GUTWIRTH, S., LEENES, R., DE HERT, P. (eds.). *Reforming European Data Protection Law.* 20. vyd. Heidelberg: Springer, 2015, Law Governance and Technology Series, s. 316 – 319.

42 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit., s. 27.

s dozorovým úřadem.[43] Na tomto místě je vhodné zmínit i další novou povinnost, kterou přináší GDPR, a to povinnost ohlašovat případy porušení zabezpečení ochrany osobních údajů (bezpečnostní incidenty) dozorovému úřadu a oznamovat je subjektům údajů. I tyto povinnosti jsou navázané na riziko hrozící subjektům údajů, riziko je ale posuzováno ve vztahu ke konkrétnímu bezpečnostnímu incidentu.[44]

Další z výraznějších změn, které přineslo GDPR, je zrušení obecné povinnosti správce ohlašovat zpracování osobních údajů dozorovým úřadům zakotvené jak ve Směrnici 94/46/ES, tak v ZOOÚ.[45] Jak je explicitně uvedeno v recitálu 89 GDPR, ohlašovací (oznamovací) povinnost ne vždy přispívala ke zlepšení ochrany osobních údajů a představovala spíše administrativní a finanční zátěž. Obecnou ohlašovací povinnost GDPR nahrazuje jinými postupy a mechanismy, které cílí na ty typy operací zpracování, jenž mohou být vysoce rizikové pro práva subjektů údajů. Pod tyto nové postupy a mechanismy lze podřadit např. již zmiňovanou povinnost v některých případech jmenovat pověřence pro ochranu osobních údajů, provádění preventivního posouzení vlivu operací zpracování na ochranu osobních údajů či předběžnou konzultaci zamýšleného zpracování osobních údajů s dozorovým úřadem.[46]

Z přechozích odstavců vyplývá, které nové povinnosti pro správce osobních údajů přineslo GDPR. Co se týče práv subjektů údajů, lze učinit závěr, že GDPR převzalo úpravu nastolenou Směrnicí 95/46/ES s tím, že ji opět více rozšiřuje. Nově zavedeno je právo na přenositelnost údajů, kterému je věnován celý čl. 20 GDPR. Právo na přenositelnost údajů ve zkratce znamená, že subjekt údajů má, při naplnění určitých předpokladů, právo získat od správce svoje osobní údaje, které mu poskytnul, a předat je jinému správci bez toho, aby mu v tom „původní“ správce jakkoliv bránil. GDPR se v souvislosti s právy subjektů, na rozdíl od Směrnice 95/46/ES, zabývá např. také problematikou doložení totožnosti osoby, která uplatňuje práva, když umožňuje správci za určitých okolností požadovat po této osobě informace potvrzující totožnost subjektu údajů.[47]

Změny GDPR přináší i ohledně sankcí (správních pokut), které mají členské státy ukládat za porušení GDPR. V čl. 83 GDPR určuje obecná pravidla pro ukládání

43 Sdělení ÚOOÚ *Nové přístupy a povinnosti*, dostupné na https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=4720.
44 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 28.
45 Srov. čl. 18 Směrnice 95/46/ES a § 16 ZOOÚ.
46 MAŠTALKA, J. *Nové nařízení EU o ochraně osobních údajů a některé záležitosti spojené s jeho aplikací v ČR*. op. cit.
47 Čl. 12 odst. 6 GDPR.

správních pokut a explicitně stanoví dvě různé horní hranice peněžitých sankcí pro případy porušení vyčtených povinností. Dle významu ustanovení, která správce či zpracovatel poruší, jsou v GDPR stanoveny horní hranice pokuty částkou 10.000.000 EUR (nebo až 2 % celosvětového ročního obratu jedná-li se o podnik) nebo 20.000.000 EUR (nebo až 4 % celosvětového ročního obratu u podniku).[48] V České republice se tyto horní hranice výše pokut budou vztahovat s největší pravděpodobností toliko na podnikatelské subjekty, orgánům veřejné moci a veřejným subjektům bude zřejmě možné udělit sankci v maximální možné výši 10.000.000,- Kč.[49]

Dle názoru autorky právě výše hrozících sankcí zvyšuje motivaci správců zaměřit se na analýzu dosud prováděného zpracování osobních údajů a případně též na uvedení veškerých procesů a operací, při nichž dochází k práci s osobními údaji, do souladu s právními předpisy. Až rozhodovací praxe vnitrostátních orgánů však ukáže, jaké pokuty budou za porušení jednotlivých ustanovení GDPR reálně ukládány. Zatím nejvyšší pokutu za porušení povinností dle GDPR uložil dne 21. 1. 2019 dozorový orgán Francie (CNIL) společnosti GOOGLE LLC, jednalo se o částku 50.000.000,- EUR. Důvodem pro uložení této sankce bylo porušení zásady transparentnosti, nedostatečné plnění informační povinnosti vůči subjektům údajů a absence zajištění souhlasu subjektů údajů se zpracováním jejich údajů za účelem tvorby personalizované reklamy, který by odpovídal požadavkům GDPR.[50]

Autorka se zároveň do určité míry ztotožňuje s názorem, že výše pokuty byla mnohdy využívána advokáty či jinými subjekty nabízejícími služby poradenství v oblasti GDPR k přesvědčení klientů o nutnosti provést právní analýzu a úpravu postupů při jimi prováděném zpracování osobních údajů s tím, že ale není pravděpodobné, že v praxi budou pokuty ve výši dosahující možného maxima ukládány.[51] Na druhou stranu však nebylo a není vhodné přizpůsobení postupů při zpracování osobních údajů GDPR příliš podceňovat a účinnost GDPR může v několika případech napomoci odstranit nedostatky při provádění zpracování, kterým správci a zpracovatelé dříve nepřikládali přílišný význam.

---

48 Čl. 83 odst. 4 a 5 GDPR.

49 § 60 vládního návrhu ZZOÚ, sněmovní tisk 138/0, dostupné na http://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=138&CT1=0.

50 The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. Dostupné na https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

51 Srov. VAN EIJK, N. *About Finding Practical Solutions (Without the GDPR)*. European Data Protection Law Review, Vol. 3, Issues 3 (2017), s. 310 – 312.

Stejně jako Směrnice 95/46/ES, GDPR předpokládá, že členské státy pověří alespoň jeden nezávislý orgán veřejné moci, aby vykonával funkci dozorového úřadu pro oblast ochrany osobních údajů.[52] Tímto úřadem v České republice bude ÚOOÚ[53], který je ústředním správním úřadem pro oblast ochrany osobních údajů již od účinnosti ZOOÚ.

Poslední změna nastolená GDPR, která bude v této kapitole nastíněna, je zrušení pracovní skupiny pro ochranu osobních údajů zřízené čl. 29 Směrnice 95/46/ES („WP29“) a její transformace na Evropský sbor pro ochranu osobních údajů („Sbor“).[54] Sbor je, na rozdíl od WP29, dle GDPR nadán právní subjektivitou. Je tvořen vedoucím jednoho dozorového úřadu z každého členského státu a evropským inspektorem ochrany údajů. Činnosti Sboru má právo se účastnit i Evropská komise, není jí však přiznáno hlasovací právo.[55] Úkoly Sboru jsou vymezeny v čl. 70 GDPR a náleží k nim mj. i vydávání pokynů, doporučení a osvědčených postupů pro stanovené oblasti GDPR. Dalo by se tedy říci, že Sbor dotváří GDPR výkladovými materiály, které sice nejsou pro správce závazné, nicméně mají poměrně velký význam, neboť jsou výsledkem práce zástupců dozorových úřadů, a dozorové úřady se jimi řídí. Je tedy nanejvýš vhodné, aby správci při zpracování osobních údajů zohledňovaly metodické pokyny vydané WP29 a Sborem.[56]

Vzhledem k tomu, že s vydáváním doporučení a postupů k GDPR započala již WP29 (WP29 od roku 2016 vydává „Guidelines“), ke dni zřízení Sboru existovalo několik validních dokumentů sloužících jako výkladový materiál k GDPR, Sbor tyto během své první plenární schůze schválil a prezentuje je jako relevantní metodické pokyny k GDPR. Během první plenární schůze Sbor také výslovně potvrdil návaznost na práci WP29.[57]

GDPR jako celek bývá někdy označováno jako revoluční pro práva subjektů osobních údajů a povinnosti správců. Byť nelze pominout, že GDPR přináší řadu novinek, které budou mít nezanedbatelný dopad zejména pro správce (zejména nastolení výše popsaných nových povinností správce), autorka se ztotožňuje s názorem vysloveným ÚOOÚ, že označovat GDPR jako revoluci v právní úpravě ochrany

52 Čl. 51 odst. 1 GDPR.
53 § 48 vládního návrhu ZZOÚ.
54 Recitál 139 GDPR a čl. 68 GDPR.
55 Čl. 68 odst. 1, 3 a 5 GDPR.
56 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 30.
57 *Endorsement of GDPR WP29 Guidelines (Endorsement 1/2018)* dostupné na https://edpb.europa.eu/node/89.

osobních údajů není přiměřené. GDPR nepřináší převrat v úpravě ochrany osobních údajů, ale spíše rozšiřuje stávající právní úpravu, jedním ze znaků GDPR je ostatně návaznost na Směrnici 95/46/ES co do sledovaných cílů a zásad ochrany osobních údajů.[58]

Závěrem je vhodné doplnit, že GDPR nebylo jediným předpisem, který byl na úrovni EU přijat v souvislosti s reformou rámce pro ochranu osobních údajů. V rámci tzv. balíčku opatření pro reformu ochrany údajů byla přijata též Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV („trestněprávní směrnice o ochraně osobních údajů“).[59] Reforma právního rámce ochrany osobních údajů na úrovni EU zahrnuje dále také přijetí Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. Dopad obou zmíněných směrnic na „běžné“ správce či zpracovatele osobních údajů ale bude minimální, neboť se týkají specifických oblastí zpracování osobních údajů v rámci trestního řízení, resp. předávání evidence cestujících orgánům veřejné moci ze strany leteckých dopravců.[60]

1.3 Právní úprava ochrany osobních údajů v ČR

Základy pro právní úpravu ochrany soukromí i osobních údajů v právním řádu České republiky lze nalézt již v rámci ústavního pořádku, a to v Listině základních práv a svobod („LZPS“). Relevantní pro danou oblast jsou zejména čl. 7 a čl. 10 LZPS. Čl. 7 odst. 1 LZPS stanoví, že *„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“* Čl. 10 LZPS pak do určité míry konkretizuje čl. 7 a garantuje každému jedinci právo na ochranu lidské důstojnosti, cti, dobré pověsti a jména, dále právo na ochranu před neoprávněným zásahem do soukromého a rodinného života a na ochranu před zneužíváním údajů o svojí osobě.

58 Srov. Dokument ÚOOÚ *Desatero omylů*, dostupné na https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=4818&n=desatero-omylu&p1=3938.
59 Sdělení Komise Evropskému parlamentu a Radě ze dne 16. 8. 2018, COM(2018) 43 final/2, op. cit.
60 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 16.

Do určitého rozporu s čl. 10 LZPS se však dostává čl. 17 LZPS, který zakotvuje svobodu projevu a právo na informace. Jako konkrétní příklad rozporu lze uvést čl. 10 odst. 3, který stanoví právo každého *„na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“*, proti kterému stojí znění čl. 17 odst. 2 *„každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.“* Ochranu soukromí garantovanou čl. 7 a 10 LZPS tak nelze považovat za neomezenou a neomezitelnou. Vyplývá-li z čl. 7 a 10 LZPS, že ochrana soukromí má být zaručena proti neoprávněným zásahům, je zřejmé, že existují i zásahy oprávněné mající základ např. právě v čl. 17 LZPS.[61]

Je vhodné na tomto místě poukázat na to, že konflikt základních lidských práv a svobod není obecně ničím výjimečným. Často může dojít ke střetu svobody, soukromí, lidské důstojnosti na straně jedné a ochrany vlastnictví, života, bezpečnosti na straně druhé.[62]

Návod, jak postupovat v případě, že dojde k takovému konfliktu dvou proti sobě stojících základních práv či svobod, poskytnul i Ústavní soud ČR v nálezu Pl. ÚS 4/94 ze dne 12. října 1994. Jedná se o známý test proporcionality, jehož podstatou je poměřování základních práv či svobod, které stojí ve vzájemné kolizi, s cílem určit, které právo nebo svoboda může být omezena na úkor jiného práva či svobody, tedy které právo nebo svoboda má v daném případě přednost. Poměřování základních práv a svobod je založeno na třech kritériích. Prvním je kritérium vhodnosti, kdy je nutné nalézt odpověď na otázku, zda institut omezující určité základní právo je způsobilý dosáhnout sledovaného cíle. Druhým kritériem je potřebnost, tedy porovnání legislativního prostředku, který omezuje základní právo nebo svobodu, s jinými prostředky, které by umožnily dosáhnout totožného cíle, ale nezasahovaly by do základních práv a svobod. Posledním kritériem je porovnání závažnosti v kolizi stojících základních práv.

Co se týče zákonné úpravy, na prvním místě je příhodné uvést zákon č. 89/2012 Sb., občanský zákoník, („OZ“), který garantuje právo na ochranu soukromí či ochranu osobnosti člověka. Již v úvodních ustanoveních OZ deklaruje právo každého na ochranu života, zdraví, svobody, cti, důstojnosti a soukromí.[63] V hlavě II. OZ je přitom celý

61 MAŠTALKA, J. *Osobní údaje, právo a my. 1. vydání*, op. cit. s. 6.
62 MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích. 1. vydání*, op. cit. s. 65.
63 § 3 odst. 2 písm. a) OZ.

oddíl věnovaný ochraně osobnosti člověka, zahrnující mj. ochranu podoby člověka a jeho soukromí či právo na duševní a tělesnou integritu.[64]

Prvním zákonem, který řešil přímo otázku ochrany osobních údajů při jejich zpracování, přijatým na území České republiky byl již zmiňovaný zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Jak již plyne ze samotného názvu tohoto zákona, dotýkal se výlučně zpracování osobních údajů v informačních systémech, nikoliv zpracování údajů v papírových evidencích, které v 90. letech stále převažovaly.[65]

Prvním komplexním zákonem upravujícím ochranu osobních údajů se tak stal ZOOÚ, který nabyl účinnosti dne 1. června 2000 (s výjimkou tří §§, které nabyly účinnosti až 1. prosince 2000) a je účinný dodnes. ZOOÚ byl po dobu svojí účinnosti několikrát novelizován, významnější novelizací ZOOÚ prošel v roce 2004, a to z důvodu nutnosti transponovat Směrnici 95/46/ES v souvislosti se vstupem České republiky do EU.[66]

ZOOÚ se vztahuje na veškeré zpracování osobních údajů prováděné orgány veřejné moci i fyzickými a právnickými osobami s výjimkou nahodilého shromažďování údajů a zpracování údajů prováděného fyzickou osobou výhradně pro její osobní potřebu.[67] Předmětem ZOOÚ je úprava práv a povinností v rámci zpracování osobních údajů a vymezení podmínek předávání osobních údajů do jiných států.[68] Na základě ZOOÚ byl také zřízen ÚOOÚ jako dozorový úřad pro oblast ochrany osobních údajů. Blíže upravena je i působnost a postavení ÚOOÚ, jeho organizace a činnost.[69] Hlava VII. tohoto zákona je pak věnovaná přestupkům v oblasti zpracování osobních údajů.

Zpracování osobních údajů se věnují i další zákony komplexně upravující určitou problematiku. Ve vztahu k ZOOÚ se věci úpravy ochrany osobních údajů jedná o zákony speciální. Jedním z takových zákonů je i zákoník práce, který se v některých svých ustanoveních věnuje ochraně soukromí a osobních údajů v rámci pracovněprávních vztahů. Klíčový je § 316 zákoníku práce, který se dotýká zejména ochrany soukromí zaměstnance a ochrany majetku zaměstnavatele, a upravuje výkon

64 Srov. § 81 a násl. OZ.
65 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 18.
66 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 19.
67 § 3 ZOOÚ.
68 § 1 ZOOÚ.
69 § 2 ZOOÚ a § 28 a násl. ZOOÚ.

práva kontroly ze strany zaměstnavatele a určitá pravidla pro získávání údajů o zaměstnancích.

Úpravu týkající se zpracování osobních údajů zaměstnanců zaměstnavatelem lze najít i na dalších místech zákoníku práce, za zmínku stojí např. § 96 stanovující povinnost vést u jednotlivých zaměstnanců evidenci pracovní doby, § 105 ukládající zaměstnavateli povinnost vést evidenci o úrazech zaměstnanců či § 312, který se týká vedení osobního spisu zaměstnance.

1.3.1 Vliv GDPR na národní právní úpravu

V návaznosti na reformu evropského právního rámce ochrany osobních údajů měl být ke dni účinnosti GDPR, tedy ke dni 25. května 2018, ZOOÚ zrušen a místo něj měl být přijat tzv. adaptační zákon, který připraví právní řád ČR na dopad GDPR a upraví záležitosti, o kterých GDPR stanoví, že mají být upraveny na úrovni vnitrostátního právního řádu, nebo, dle vůle zákonodárců členských států, mohou být upraveny na vnitrostátní úrovni. Adaptační zákon bude ve vztahu k GDPR doplňkovým právním předpisem, a nebude mít stejný charakter jako ZOOÚ, neboť nebude obsahovat komplexní úpravu práv a povinností souvisejících se zpracováním osobních údajů.

K dnešnímu dni však takový zákon nebyl přijat, nicméně vládní návrh zákona o zpracování osobních údajů („ZZOÚ“) byl ke dni 2. 4. 2019 již předložen prezidentovi republiky k podpisu. ZZOÚ kromě adaptace právního řádu České republiky na GDPR také transponuje trestněprávní směrnici o ochraně osobních údajů. ZZOÚ tedy s největší pravděpodobností nabyde účinnosti jen těsně před uplynutím jednoho roku od účinnosti GDPR.

V oblasti právní úpravy ochrany osobních údajů v České republice stále panuje nežádoucí stav, kdy GDPR již nabylo účinnosti, zároveň je stále účinný ZOOÚ a adaptační zákon předvídaný GDPR (ZZOÚ) nebyl do dnešního dne přijat.

I několik měsíců po účinnosti GDPR se tedy stále nabízela otázka, jakými předpisy na ochranu osobních údajů se v tomto „mezidobí“ mají správci, zpracovatelé a subjekty údajů řídit a jakým způsobem mají tyto předpisy aplikovat a vykládat. K zodpovězení této otázky je nutné se zaměřit na základní pravidla aplikace právních aktů EU v členských státech a jejich případného konfliktu s vnitrostátními právními normami.

Jak již bylo uvedeno výše, GDPR je jakožto nařízení přímo použitelné v členských státech EU. Již od jeho účinnosti se tedy bude na území ČR na zpracování osobních údajů bez dalšího aplikovat. GDPR v zásadě přebírá hmotněprávní roli ZOOÚ, a v rozsahu stanovení práv a povinností při zpracování osobních údajů nahrazuje ZOOÚ.[70] To ale samo o sobě úplně nevylučuje aplikaci doposud účinných tuzemských právních předpisů upravujících oblast ochrany osobních údajů (zejména ZOOÚ), ty však budou muset být používány a vykládány vždy v souladu s GDPR. Jinými slovy platí, že pokud je určitý aspekt upraven jak v GDPR, tak v ZOOÚ, ode dne účinnosti GDPR se použije úprava obsažená v GDPR. Pokud je určitá problematika upravena v ZOOÚ nad rámec GDPR a zároveň úprava obsažená v ZOOÚ není v rozporu s GDPR, je možné aplikovat ZOOÚ (souladně s GDPR).

Problém případného existujícího rozporu mezi úpravou obsaženou v GDPR a vnitrostátním předpisem lze vyřešit použitím jedné ze základních zásad práva EU, a to zásady aplikační přednosti práva EU. Tato zásada byla formulována Soudním dvorem EU v rozhodnutí ve věci 6/64 Flaminio Costa vs. E.N.E.L. a stanoví, že pokud se přímo použitelná norma práva EU dostane do aplikační kolize s vnitrostátní normou, má norma práva EU aplikační přednost.

Národní předpisy však kvůli svému rozporu s právními normami EU nejsou automaticky nicotné a zůstávají součástí právního řádu daného členského státu. Tento závadný stav představuje narušení právní jistoty adresátů právních norem, a měl by být proto zákonodárci členských států vždy odstraněn, veškeré vnitrostátní normy by tedy měly být v souladu s legislativou EU.

70 Dokument ÚOOÚ *Základní příručka k GDPR*. Dostupné na https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744.

2 Vymezení základních pojmů

Účelem této kapitoly je vymezení některých klíčových pojmů týkajících se ochrany osobních údajů. Níže v kapitole není uveden kompletní výčet pojmů, které mají svůj význam v oblasti práva na ochranu osobních údajů, ale pouze ty pojmy, které autorka považuje za důležité, a zároveň jsou dále používány v diplomové práci. Vymezení základních pojmů vychází zejména z právní úpravy obsažené v aktuálním znění GDPR, pro přehled je dále v některých případech uvedeno srovnání s právní úpravou obsaženou ve Směrnici 95/46/ES zrušené GDPR, resp. v ZOOÚ. Úvodem je nicméně třeba konstatovat, že, co se týče pojetí základních pojmů, nedošlo s účinností GDPR k nijak zásadním změnám.

2.1 Osobní údaj

Pojem osobní údaj je v rámci práva na ochranu osobních údajů zcela zásadní, neboť vymezuje oblast působnosti právní regulace. Lze tedy říci, že údajům, které nemají kvalitu osobního údaje, nebude poskytnuta ochrana dle GDPR.[71] Jinými slovy platí, že aby mohla být údajům, resp. jejich subjektům poskytnuta právní ochrana, je nutné v prvé řadě učinit závěr o tom, zda se vůbec jedná o osobní údaj. V opačném případě se právní úprava na ochranu osobních údajů nebude aplikovat.

V čl. 4 GDPR je k pojmu osobní údaj uvedeno následující: *„osobními údaji (se rozumí) veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*“

Definice osobního údaje obsažená v GDPR se nijak zásadně neliší od definic uvedených ve Směrnici 95/46/ES a v ZOOÚ, když dle § 4 písm. a) ZOOÚ platí, že *„osobním údajem (se rozumí) jakákoliv informace týkající se určeného nebo určitelného subjektu údajů“* a v čl. 2 Směrnice 95/46/ES je obsažena tato definice

71 PINKAVOVÁ, A., FOŘT, F. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. Praha: Leges, 2018, s. 51, ISBN 978-80-7502-288-2.

osobního údaje: *„osobními údaji“ (se rozumí) veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů)“*. Stejně jako v definici osobního údaje dle čl. 4 GDPR pak i v definicích osobního údaje dle ZOOÚ a Směrnice 95/46/ES následuje demonstrativní výčet těch informací, pomocí nichž je možné fyzickou osobu identifikovat (tzv. identifikátorů).

V čl. 4 GDPR je však, oproti Směrnici 95/46/ES a ZOOÚ, uveden širší výčet identifikátorů. Nově jsou v definici pojmu osobní údaj jako identifikátory explicitně uvedeny též lokační údaje či síťový identifikátor (např. IP adresa nebo cookies) nebo jeden či více zvláštních prvků genetické identity fyzické osoby. Rozšíření demonstrativního výčtu identifikátorů lze považovat za jedinou výraznější změnu v definici pojmu osobní údaj, ke které došlo spolu s účinností GDPR.

Autorka však považuje za podstatné zmínit, že ačkoliv došlo k rozšíření demonstrativního výčtu identifikátorů, nelze toto považovat za rozšíření samotné definice pojmu osobní údaj. I na základě původní definice osobního údaje totiž byly kategorie údajů, které jsou dnes v GDPR výslovně uvedeny (např. dynamická IP adresa), považovány v určitých případech za osobní údaje.[72] Tento názor vyslovil i SDEU ve svém rozhodnutí ve věci C-582/14 ze dne 19. 10. 2016. SDEU v tomto rozhodnutí mj. učinil závěr, že dynamická IP adresa je pro poskytovatele online mediálních služeb uchovávajícího tuto adresu v souvislosti s přístupem osoby na internetovou stránku zpřístupněnou veřejnosti osobním údajem ve smyslu Směrnice 95/46/ES za předpokladu, že tento poskytovatel služeb má k dispozici právní prostředky umožňující nechat subjekt údajů identifikovat, a to díky dalším informacím, které má k dispozici poskytovatel internetového připojení tohoto subjektu.[73]

Samotný pojem osobní údaj a jednotlivé části definice tohoto pojmu detailně zpracovává též stanovisko WP29 č. 4/2007, k pojmu osobní údaj, které je možné považovat za relevantní i po účinnosti GDPR. Toto stanovisko člení definici pojmu osobní údaj na čtyři hlavní složky.

První složka zahrnující dílčí pojem „veškeré informace“ zřetelně odkazuje na úmysl zákonodárce stanovit široké pojetí pojmu osobní údaj. Z hlediska povahy informací platí, že pojem osobní údaj zahrnuje jak objektivní informace o osobě (např. výška, barva vlasů), tak subjektivní informace (typicky názory či hodnocení). Pro účely

72 PINKAVOVÁ, A., FOŘT, F. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobníc údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. op. cit. s. 52.
73 Rozsudek SDEU ze dne 19. října 2016, Patrick Breyer proti Spolkové republice Německo, věc C-582/14, EU:C:2016:779.

definice pojmu osobní údaj přitom není podstatné, zda jsou tyto objektivní či subjektivní informace o osobě pravdivé nebo prokázané. Obsahem informací mohou být údaje libovolného typu, např. údaje ze soukromého a rodinného života v úzkém smyslu, informace o pracovních vztazích, ekonomickém nebo společenském chování. Libovolný může být též formát a nosič informací.[74] Široké pojetí pojmu osobní údaj podpořil i Soudní dvůr Evropské unie v rozhodnutí ve věci C-101/01 ze dne 6. listopadu 2003.[75]

Druhou a zásadní složkou definice pojmu osobní údaj je vztah mezi informacemi a osobou. Informace definovaná výše se totiž musí týkat jednotlivce (musí být „o" tomto jednotlivci), aby mohla být považována za osobní údaj.[76] WP29 se již ve svém starším stanovisku podrobněji věnovala otázce definice souvislosti mezi informací a jednotlivcem a dospěla k závěru, že určité informace lze pokládat za informace týkající se jednotlivce za předpokladu, že se vztahují k totožnosti, charakteristickým znakům či chování jednotlivce nebo pokud je možné tyto informace využít k určení nebo ovlivnění způsobu, jakým bude s jednotlivcem zacházeno, nebo jakým bude jednotlivec hodnocen.[77] S ohledem na výše uvedené WP29 dovozuje, že aby mohly být informace považovány za takové, které souvisejí s jednotlivcem, má být přítomen alternativně jeden z těchto prvků: obsah (informace se podávají o jednotlivci, tedy se týkají jednotlivce ve smyslu běžného chápání pojmu „týkat se"), účel (účelem používání informací je hodnocení jednotlivce nebo ovlivnění jeho postavení či chování), výsledek (použití informace bude mít zřejmě dopad na práva a oprávněné zájmy jednotlivce).[78]

Třetím prvkem je „identifikovaná nebo identifikovatelná" (fyzická osoba). V obecné rovině dle WP29 platí, že fyzická osoba může být považována za identifikovanou, pokud ji v určité skupině lze odlišit od ostatních členů takové skupiny. Identifikovatelná je pak fyzická osoba v případě, že je možné ji identifikovat, ačkoliv tak prozatím nebylo učiněno. Identifikaci lze provést prostřednictvím v této kapitole již zmíněných identifikátorů, jejichž demonstrativní výčet je uveden jak ve Směrnici 95/46/ES, v ZOOÚ, tak v GDPR.[79]

Čtvrtou složkou je (fyzická) „osoba". Právo na ochranu osobních údajů se vztahuje na všechny fyzické osoby (lidi). Jedná se o právo univerzální, které se

74 WP29: Stanovisko č. 4/2007*, k pojmu osobní údaj*, přijaté dne 20. června 2007.
75 Rozsudek SDEU ze dne 6. listopadu 2003, Bodil Lindqvist proti Švédsku, věc C-101/01, EU:C:2003:596.
76 Stanovisko WP29 č. 4/2007, *k pojmu osobní údaj*.
77 Working Party document No WP 105: "*Working document on data protection issues related to RFID technology*", přijatý dne 19. 1. 2005.
78 WP29: Stanovisko č. 4/2007, *k pojmu osobní údaj*, op. cit.
79 Tamtéž.

neomezuje pouze na státní příslušníky či obyvatele určité země.[80] Toto pojetí navazuje na čl. 6 Všeobecné deklarace lidských práv, dle kterého platí, že: *„Každý má právo na to, aby byla všude uznávána jeho právní osobnost.“* Skutečnost, že právo na ochranu osobních údajů se dotýká pouze fyzických osob, však neznamená, že se pravidla ochrany osobních údajů nemohou v určitých případech nepřímo vztahovat i na údaje související s právnickými osobami, typickým příkladem je obchodní firma právnické osoby odvozená od jména fyzické osoby, nebo podnikový e-mail, který obsahuje obchodní firmu dané společnosti a užívá jej konkrétní zaměstnanec. V tomto případě půjde o údaje, jejichž obsah se týká právnické osoby.[81]

2.1.1 Zvláštní kategorie osobních údajů

Směrnice 95/46/ES stejně jako GDPR uvádí výčet kategorií osobních údajů, které jsou označeny jako zvláštní, a kterým je jako takovým přiznán specifický režim právní ochrany.[82] Přiznání zvláštního a přísnějšího režimu právní ochrany některým kategoriím osobních údajů je odůvodněno jejich povahou, když platí, že zpracování takových údajů může zásadně ohrozit základní právo subjektů údajů na soukromí.[83] V ZOOÚ je, po vzoru Směrnice 95/46/ES, také uveden výčet kategorií osobních údajů, které podléhají přísnějšímu režimu zpracování.[84] Tento výčet je svoji povahou taxativní[85]. ZOOÚ pro tyto osobní údaje užívá pojem „citlivé osobní údaje“. Pojem „citlivé osobní údaje“ GDPR zavádí jako zkratku pro zvláštní kategorie osobních údajů.[86] Autorka považuje za vhodné na tomto místě zmínit, že ZZOÚ s pojmem „citlivý osobní údaj“ již neoperuje.[87]

Konkrétní výčet zvláštních kategorií osobních údajů je uveden v čl. 9 GDPR. Tento článek stanoví, že se jedná o osobní údaje, *„které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém*

80 WP29: Stanovisko č. 4/2007*, k pojmu osobní úda*j, op. cit.
81 Tamtéž.
82 Srov. čl. 8 Směrnice 95/46/ES a čl. 9 GDPR.
83 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR, 2017, s. 162, ISBN 978-80-7552-765-3.
84 Srov. § 4 písm. b) ZOOÚ.
85 KUČEROVÁ, A., NOVÁKOVÁ L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář. 1.* vydání. Praha: C. H. Beck, 2012, s. 54, ISBN 978-80-7179-226-0.
86 Recitál 10 GDPR.
87 Srov. § 64 odst. 6 ZZOÚ, Parlament ČR, Poslanecká sněmovna, 8. volební období, sněmovní tisk č. 138/0 a důvodová zpráva k ZZOÚ.

přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby." Při porovnání výčtu zvláštních kategorií v GDPR s výčtem uvedeným ve Směrnici 95/46/ES lze dospět k závěru, že GDPR tuto kategorii rozšiřuje o genetické a biometrické údaje a dále, kromě údajů týkajících se sexuálního života, zařazuje do zvláštní kategorie osobních údajů výslovně též údaj o sexuální orientaci.

Co se týče české právní úpravy, je nutné uvést, že ZOOÚ na genetické i biometrické údaje již pamatoval a zahrnul je do výčtu citlivých osobních údajů v odst. 4 písm. b). Mezi pojetím biometrických údajů jako citlivých osobních údajů v ZOOÚ a v GDPR je možné nalézt drobný rozdíl, když dle ZOOÚ jsou k citlivým údajům zařazeny biometrické údaje, které jsou používány k identifikaci nebo autentizaci subjektu údajů. GDPR k zařazení mezi zvláštní kategorie osobních údajů vyžaduje, aby byly biometrické údaje využity jen pro identifikaci. I přesto, že jsou procesy autentizace a identifikace z pohledu informační bezpečnosti odlišné, lze dovodit, že správce, který využije biometrické údaje k autentizaci, má obvykle možnost tyto využít též k identifikaci. Důsledek výše popsané změny pojetí biometrických údajů v praxi tedy není zcela zásadní.[88]

Při porovnání stále platné a účinné národní právní úpravy ochrany osobních údajů a s GDPR, je třeba dále zmínit, že v ZOOÚ, stejně jako ve Směrnici 95/46/ES, chyběl ve výčtu citlivých údajů údaj o sexuální orientaci. Nad rámec výčtu obsaženém v GDPR naopak ZOOÚ mezi citlivé údaje řadí i údaj o národnostním původu. Obdobně též ZOOÚ do seznamu citlivých údajů zařadil údaj o odsouzení za trestný čin. GDPR přitom údaj o odsouzení za trestný čin sice neřadí formálně přímo mezi zvláštní kategorie osobních údajů ve smyslu čl. 9 GDPR, avšak speciálně pro tento typ osobního údaje stanoví zvláštní podmínky pro jeho zpracování. GDPR klade důraz zejména na to, aby byly osobní údaje tohoto druhu zpracovány výlučně pod dozorem orgánu veřejné moci, nebo aby bylo zpracování oprávněné dle práva EU nebo členského státu.[89]

GDPR oproti dřívější právní úpravě na ochranu osobních údajů na úrovní národní i EU nově obsahuje též vcelku podrobné definice některých konkrétních skupin zvláštních kategorií osobních údajů. Blíže se věnuje pojmu „genetické údaje", o kterých stanoví, že se jedná o takové údaje, které plynou hlavně z analýzy biologického vzorku

88 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*, op. cit. s. 163.

89 Čl. 10 GDPR.

fyzické osoby, jsou způsobilé poskytnout jedinečné informace o fyziologii či zdraví dané osoby a týkají se zděděných nebo získaných genetických znaků osoby.[90]

K „biometrickým údajům“ GDPR dále blíže uvádí, že jde o údaje, které umožňují nebo potvrzují jedinečnou identifikaci fyzické osoby s tím, že tyto údaje vyplývají z konkrétního technického zpracování a týkají se fyzických, fyziologických znaků nebo znaků chování konkrétní fyzické osoby.[91] Pro biometrické údaje je příznačné, že je lze poměrně snadno odezírat z lidského těla a mohou být zachyceny na fotografii, videu, nahrávce hlasového projevu apod. V tomto okamžiku se ale jedná o tzv. „raw data“, tedy data, která ještě nebyla zpracovaná, a nelze je sama o sobě považovat za biometrické údaje ve smyslu GDPR.[92] Aby tedy mohly být biometrické údaje považovány za zvláštní kategorie osobních údajů ve smyslu čl. 9 GDPR, musí platit, že dojde k jejich zpracování, a to za účelem jedinečné identifikace fyzické osoby.[93] To samé platí i pro údaje genetické.

Konečně za „údaje o zdravotním stavu“ GDPR považuje všechny údaje související se zdravím fyzické osoby bez ohledu na to, zda jde o zdraví duševní nebo tělesné. K údajům o zdravotním stavu GDPR dále řadí též informace o poskytnutí zdravotních služeb vypovídající o zdravotním stavu fyzické osoby.[94] Bližší specifikace informací, které lze podřadit pod pojem „údaje o zdravotním stavu“ je obsažena rovněž v recitálu 35 GDPR, ve kterém je mj. uvedeno, že pod pojem údaje o zdravotním stavu spadají údaje shromážděné o fyzické osobě během registrace pro účely poskytování zdravotní péče, informace získané během provádění testů nebo vyšetřování částí těla, tělesných látek, informace o nemoci, anamnéze, klinické léčbě apod.

S některými ze zvláštních kategorií osobních údajů se zpravidla setkáme i při zpracování osobních údajů v rámci pracovněprávních vztahů. Významná a problematická je např. otázka údajů o zdravotním stavu zaměstnance. ÚOOÚ ve svém stanovisku uvádí, že v praxi občas dochází k chybnému pochopení klasifikace údaje o zdravotním stavu jako údaje citlivého, když se zaměstnavatel mylně domnívá, že zpracovává údaj o zdravotním stavu. Typicky se jedná o případ potvrzení lékaře o tom, zda je zaměstnanec způsobilý k výkonu práce (např. potvrzení ze vstupní lékařské prohlídky). Takové potvrzení lékaře není citlivým osobním údajem o zdravotním stavu,

90 Čl. 4 odst. 13 GDPR.
91 Čl. 4 odst. 14 GDPR.
92 MATEJKA, J., KRAUSOVÁ, A., GÜTTLER, V., *Biometrické údaje a jejich právní režim*. Revue pro právo a technologie 17/2018, s. 91.
93 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 53.
94 Čl. 4 odst. 15 GDPR.

jelikož z něj nevyplývají konkrétní informace o zdravotním stavu zaměstnance, nicméně jen skutečnost, zda je či není schopen výkonu práce. Zaměstnavatel tedy v tomto případě nezpracovává citlivý osobní údaj.[95]

Jak vyplývá z výše uvedeného, za citlivý údaj o zdravotním stavu zaměstnance naopak je možné považovat např. konkrétní informace o omezení zdravotní způsobilosti zaměstnance ve vztahu k jím vykonávané práci. Tento závěr v minulosti potvrdil i SDEU v rozhodnutí ve věci C-101/01, ve kterém posuzoval otázku, zda je informace o tom, že si jedinec poranil nohu a čerpá ze zdravotních důvodů částečné volno, osobním údajem týkajícím se zdraví dle čl. 8 odst. 1 Směrnice 95/46/ES. Dle názoru SDEU taková informace je osobním údajem týkajícím se zdraví ve smyslu čl. 8 odst. 1 Směrnice 95/46/ES, neboť pojem „údaje týkající se zdraví" je třeba vykládat široce, a to tak, že zahrnuje informace týkající se všech aspektů zdraví jedince, ať již fyzických nebo psychických.[96] Závěry o pojetí údajů o zdravotním stavu zaměstnance, dle názoru autorky, obstojí i po účinnosti GDPR, a to zejména s ohledem na pojetí pojmu „údaje o zdravotním stavu" v GDPR.

Další problematickou otázkou související se zpracováním zvláštních kategorií osobních údajů v rámci pracovněprávních vztahů je zpracování údaje o členství v odborové organizaci v souvislosti se srážkami příspěvků odborové organizaci ze mzdy. Údaj o členství v odborové organizaci patří ke zvláštním kategoriím osobních údajů, a jako takový by měl podléhat přísnějším pravidlům pro zpracování dle čl. 9 GDPR. ÚOOÚ ve svém stanovisku k danému problému dovodil, že za účelem realizace dohody o srážkách ze mzdy (pro úhradu členských příspěvků členů odborových organizací) není třeba zpracovat údaj o členství zaměstnance v odborové organizaci. Zaměstnavatel je povinen zpracovat jen údaj, že zaměstnanec řádně předložil písemnou dohodu o srážkách ze mzdy příslušnému útvaru zaměstnavatele, ze které je patrné, že zaměstnanec souhlasil se srážkami ze mzdy, jaká je výše srážek ze mzdy a na jaký účet mají být srážky ze mzdy poukázány.[97] Tento závěr ÚOOÚ však může být, dle mého názoru, poněkud diskutabilní, jelikož v praxi si lze poměrně obtížně představit, že by zaměstnavatel v souvislosti se srážením příspěvků odborové organizaci ze mzdy zaměstnance, nezpracovával údaj o členství v odborové organizaci např. jakožto důvod pro provádění srážek ze mzdy. Dle mého názoru by bylo možné takové zpracování

95 ÚOOÚ: Stanovisko č. 6/2012, *Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů*.

96 Rozsudek SDEU ze dne 6. listopadu 2003, Bodil Lindqvist proti Švédsku, op. cit.

97 ÚOOÚ: Stanovisko č. 2/2001, *Zpracování citlivého osobního údaje o členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací*.

údaje o členství v odborové organizaci považovat za zpracování nezbytné pro plnění právní povinnosti v oblasti pracovního práva.

2.1.2 Pseudonymizované a anonymizované osobní údaje

GDPR nově ve svém textu výslovně uvádí pojem pseudonymizace, kterým se podle čl. 4 odst. 5) GDPR rozumí takové zpracování osobních údajů, v jehož důsledku již údaje nemohou být přiřazeny ke konkrétnímu subjektu údajů bez užití dodatečných informací, za předpokladu, že takové informace jsou uchovávány odděleně a vztahují se na ně technická a organizační opatření zajišťující, že nedojde k jejich přiřazení k subjektu údajů. Jak vyplývá z recitálu 26 GDPR, údaje, které prošly procesem pseudonymizace a mohou být přiřazeny subjektu nepřímo, na základě dodatečných informací, lze označit jako údaje pseudonymizované.

Proces pseudonymizace je jedním z možných technických opatřeních dle čl. 32 odst. 1 GDPR, resp. čl. 25 odst. 1 GDPR, které slouží k zajištění zabezpečení osobních údajů. Ze znění recitálu 28 GDPR je možné dovodit, že hlavním cílem pseudonymizace má být omezení rizik pro subjekty při zpracování jejich osobních údajů a zároveň nápomoc správcům a zpracovatelům k plnění jejich povinností.

Jako praktický příklad procesu pseudonymizace lze uvést následující. V databázi se jménu a příjmení určitého jedince přidělí kód s tím, že bude odděleně uchovávána informace o tom, že konkrétní kód odpovídá konkrétnímu jménu a příjmení. Po pseudonymizaci tedy např. údaje „Josef Dvořák, učitel“ budou změněny na údaje „5F6D22, učitel“, s tím, že údaj o tom, že kód 5F6D22 je přiřazen právě Josefu Dvořákovi, je uchováván separátně (buď přímo správcem, nebo třetí osobou). Pokud by ale došlo ke spojení separátně uchovávaných informací, bude stále možné zjistit, že kódu 5F6D22 odpovídá Josef Dvořák. Ze shora uvedeného vyplývá, že i po pseudonymizaci se bude jednat o osobní údaje, které náleží do působnosti GDPR, a to právě díky existující možnosti spojení zvlášť uchovávaných informací.[98] Tento závěr plyne i z již zmiňovaného recitálu 26 GDPR.

Od údajů pseudonymizovaných je nutné odlišit údaje anonymizované, které jsou výsledkem procesu anonymizace. Hlavní rozdíl mezi oběma výše uvedenými skupinami údajů tkví zejména ve vratnosti procesu, jehož výstupem dané údaje jsou. Jak již bylo

98 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., 2017, *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*, op. cit. s. 87.

uvedeno výše, proces pseudonymizace je založen na odděleném uchovávání dodatečných informací (tzv. identifikátorů) od ostatních osobních údajů, tyto identifikátory je ale možné za použití určitých technických prostředků (např. šifrovacích klíčů) opět spojit, a je tak možné je přiřadit k subjektu údajů. Naopak v rámci procesu anonymizace jsou všechny identifikátory nevratně vymazány, a subjekt údajů přestane být navždy identifikovatelný.[99] GDPR se z tohoto důvodu na anonymizované údaje nevztahuje. Stejně tak do působnosti GDPR nenáleží anonymní informace, neboli informace, které se subjektu údajů vůbec nedotýkají.[100]

2.2 Subjekt údajů

Další ze základních pojmů souvisejících se zpracováním osobních údajů je pojem subjekt osobních údajů („subjekt údajů“). Dle čl. 4 odst. 1 GDPR je subjektem údajů jakákoliv identifikovaná nebo identifikovatelná fyzická osoba, tedy osoba, jíž je možné přímo či nepřímo identifikovat za pomocí různých identifikátorů (jméno, identifikační číslo, apod.). Zcela logicky se, stejně jako v případě pojmu osobní údaje, definice pojmu subjekt údajů v GDPR, nijak zásadně neliší od definic obsažených ve Směrnici 95/46/ES a v ZOOÚ.

Jedním z diskutovaných témat za účinnosti Směrnice 95/46/ES a ZOOÚ bylo, zda se právní předpisy na ochranu osobních údajů vztahují i na zemřelé osoby a na fyzické osoby podnikající. Ve Směrnici 95/46/ES ani v ZOOÚ nebylo výslovně stanoveno, zda se vztahují i na zemřelé osoby, nebo nikoliv. K této problematice se později vyjádřil ÚOOÚ v jednom ze svých stanovisek, kde rozlišuje dvě rozdílné skupiny ustanovení ZOOÚ, z nichž jedna zůstává platná i po smrti subjektu údajů a druhá po smrti subjektu údajů platnosti pozbývá. ÚOOÚ dospěl k závěru, že po smrti fyzické osoby platnosti pozbydou ta ustanovení ZOOÚ, ve kterých subjekt údajů vystupuje jako účastník občanskoprávních vztahů; jedná se o ustanovení upravující práva subjektů údajů a povinnosti správce ve vztahu k subjektu údajů. Na druhé straně ustanovení ZOOÚ, ve kterých subjekt údajů nevystupuje jako účastník občanskoprávních vztahů, zůstanou platná i po jeho smrti.[101] Byla tedy vyjádřena jakási dvojkolejnost pro aplikaci právní úpravy na ochranu osobních údajů na zemřelé osoby.

99 PATTYNOVÁ, J. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobníc údajů (GDPR). Data a soukromí v digitálním světě. Komentář*, op. cit. s. 69.
100 Srov. recitál 26 GDPR.
101 ÚOOÚ: Stanovisko č. 4/2012, *Zpracování osobních údajů zemřelých osob*.

Posun v otázce možnosti vztahovat právní úpravu na ochranu osobních údajů na zemřelé osoby přináší GDPR. V recitálu 27 GDPR je totiž explicitně uvedeno, že se nevztahuje na osobní údaje zesnulých osob, zároveň ale nevylučuje, aby členské státy určily vlastní pravidla ve vztahu ke zpracování osobních údajů zesnulých. Ze znění návrhu ZZOÚ plyne, že Česká republika tuto možnost nevyužila. V rámci České republiky tedy otázku, zda je zemřelá osoba subjektem právních předpisů na ochranu osobních údajů, s největší pravděpodobností nadále nebude třeba považovat za problematickou.

Z výše uvedené definice subjektu údajů je evidentní, že právní úprava na ochranu osobních údajů se nevztahuje na osoby právnické, to samozřejmě nevylučuje, aby ochraně podléhaly fyzické osoby, které jsou členy orgánů právnické osoby. Vyloučení aplikace úpravy na právnické osoby je zakotveno i v recitálu 14 GDPR.

Komplikovanější je situace u fyzických osob podnikajících, kdy sice není pochyb o tom, že fyzické osoby podnikající jsou subjekty údajů, když v § 4 písm. a) ZOOÚ je výslovně uvedeno, že *subjekt údajů se považuje za určený nebo určitelný i v případě, jestliže jej lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho ekonomickou identitu*, ale může být sporné, v jakém rozsahu se má právní úprava na ochranu osobních údajů vztahovat na zpracování osobních údajů fyzických osob podnikajících.[102] Tento závěr lze považovat jako relevantní i po účinnosti GDPR, jelikož zvláštní prvek ekonomické identity je i v čl. 4 odst. 1 GDPR uveden jako jeden z identifikátorů.

Některé údaje, které se k fyzickým osobám vztahují, totiž vypovídají pouze o jejich profesním životě (např. identifikační číslo fyzické osoby podnikající, místo výkonu profese), jiné údaje dopadají i na soukromý život (jméno, datum narození, podpis).[103] K dané problematice se vyjádřil i Ústavní soud v nálezu z roku 2004 sp. zn. Pl. ÚS 38/02, a to v tom smyslu, že ochraně dle ZOOÚ nepodléhají údaje o podnikatelské činnosti fyzických osob podnikajících stejně jako je tomu u právnických osob. Tento závěr ale není v souladu se závěry učiněnými evropskými soudy, které zdůrazňují úzkou provázanost profesního a soukromého života u fyzických osob podnikajících. Názor, že i údaje o profesní činnosti fyzické osoby podléhají ochraně osobních údajů, potvrdil např. i SDEU v rozsudku ze dne 9. listopadu 2010 ve

102 FOLDOVÁ, V. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D, *Zákon o ochraně osobních údajů. Komentář. 1. vydání,* op. cit. s. 66.

103 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*, op. cit. s. 80 - 81. q

spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Hessensku*. Evropskou judikaturu později reflektovaly i české soudy.[104]

Ve stanovisku č. 3/2011 se k dané věci vyslovil také ÚOOÚ, který se přiklání k názoru, že ZOOÚ se vztahuje na fyzické osoby podnikající a v zásadě na všechny informace, které se jich týkají (tedy jak informace o profesní činnosti, tak informace dopadající na soukromý život).

Ani v GDPR není vyjasněna aplikace úpravy na fyzické osoby podnikající, bude však v zásadě možné se i nadále opírat o judikaturu evropských i vnitrostátních soudů věnující se dané problematice.

2.3 Zpracování osobních údajů

Dalším z klíčových pojmů v oblasti ochrany osobních údajů je zpracování osobních údajů. Povinnosti stanovené právními předpisy na ochranu osobních údajů se totiž budou vztahovat jen na nakládání s osobními údaji, které je zpracováním ve smyslu těchto právních předpisů. Co se týče definice pojmu zpracování osobních údajů, GDPR opět v podstatě převzal její znění ze Směrnice 95/46/ES, a v čl. 4 odst. 2 stanoví, že zpracování osobních údajů znamená operaci nebo soubor operací s osobními údaji prováděné automatizovaným i neautomatizovaným postupem. V tomtéž článku je pak dále obsažen demonstrativní výčet konkrétních operací, které lze považovat za zpracování ve smyslu GDPR. Jedná se např. o shromáždění, zaznamenání, uložení, zpřístupnění či výmaz nebo zničení.

Ze shora uvedené definice plyne, že zpracování je operace prováděná s osobními údaji. Za operaci s osobními údaji je přitom možné považovat cokoliv, při čem správce pracuje s osobními údaji nebo s nimi nakládá či je ovlivňuje. Nehraje roli, zda správce provede více operací (úkonů) s osobními údaji, nebo zda se bude jednat o jedinou operaci. Obecně lze ale předpokládat, že pokud jsou osobní údaje ve sféře vlivu správce, bude s nimi provádět více operací než jednu – typicky údaje nejdříve shromáždí, poté je uloží, použije či zpřístupní a nakonec provede výmaz nebo zničení údajů.[105] Operace s osobními údaji mohou být prováděny automatizovanými i jinými postupy, mohou být

104 Srov. rozsudek NSS sp. zn. 1 Afs 60/2009.

105 POSPÍŠIL D. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář. 1. vydání.* op. cit. s. 68.

tedy realizovány technickými prostředky (především s využitím výpočetní techniky) i manuálně.[106]

Ne každý případ, kdy určitá osoba přistoupí k osobním údajů, však znamená zpracování osobních údajů ve smyslu výše uvedené definice. Jako příklad, kdy se o zpracování osobních údajů jednat nebude, je možné uvést ad hoc přístup k údajům nezbytný k údržbě poskytovaného hardwaru nebo softwaru. Pro rozlišení, kdy se o zpracování osobních údajů jedná a kdy nikoliv, je klíčový účel činnosti, při které dochází ke střetu s údaji. Pokud je účelem dané činnosti práce s daty jako taková, bude se jednat o zpracování, jestliže je ale přístup k údajům jen nepravidelným a nahodilým důsledkem jiné aktivity (např. údržba technických prostředků sloužících pro zpracování dat, při které může někdy dojít k přístupu k údajům), nebude se jednat o zpracování osobních údajů.[107]

Zvláštní formou zpracování nově definovanou v GDPR je profilování neboli automatizované *zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě.*[108] Profilování je charakterizováno třemi prvky: obligatorně se jedná o automatizovaný způsob zpracování, provádí se na základě osobních údajů a jeho cílem je hodnocení osobních aspektů fyzické osoby. Profilování je často užíváno k vytváření úsudků o jedincích s tím, že jsou využívány údaje z různých zdrojů s cílem učinit závěry o konkrétní osobě na základě kvalit jiných lidí, kteří jsou statisticky podobní.[109]

Specifická pravidla stanoví GDPR pro zpracování zvláštních kategorií osobních údajů, když v čl. 9 odst. 1 a priori zakazuje zpracování osobních údajů těchto kategorií. Zákaz zpracování se ale nevztahuje na případy vyčtené v odst. 2 téhož článku, těmi jsou např. udělení souhlasu se zpracováním takových osobních údajů pro určité účely, nutnost zpracování za účelem plnění povinností a výkonu zvláštních práv správce nebo subjektu v oblasti pracovního práva a práva sociálního zabezpečení, nezbytnost zpracování z důvodu veřejného zájmu v oblasti veřejného zdraví či případ, kdy se jedná o zpracování údajů, které již byly subjektem zjevně zveřejněny. Za situace, kdy je správcem prolomen zákaz zpracování zvláštních kategorií osobních údajů dle některého

106 BARTÍK V., JANEČKOVÁ E.: *Zákon o ochraně osobních údajů s komentářem*, Olomouc: ANAG, 2010, s. 45, ISBN 978-80-7263-613-6.

107 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*, op. cit. s. 86.

108 Čl. 4 odst. 4 GDPR.

109 WP29: *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*, přijaté dne 3. října 2017, ve znění naposledy revidovaném a přijatém dne 6. února 2018.

z bodů uvedených v čl. 9 odst. 2, platí, že správce musí v souladu se zásadou zákonnosti také mít právní důvod pro zpracování dle čl. 6 odst. 1 GDPR.[110]

Takřka totožnou definici zpracování osobních údajů obsahuje i ZOOÚ v § 4 písm. e) s tím, že oproti Směrnici 95/46/ES a GDPR obsahuje navíc výslovně prvek systematičnosti operací s osobními údaji. V § 4 ZOOÚ jsou dále uvedeny definice určitých operací s osobními údaji, a to shromažďování, uchovávání, blokování a likvidace.

V souvislosti s pojmem zpracování osobních údajů, resp. s vymezení, co vše je možné považovat za zpracování osobních údajů, autorka považuje za vhodné zmínit rozsudek SDEU ve věci C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ve kterém jsou uvedeny mj. závěry, že za zpracování osobních údajů ve smyslu Směrnice 95/46/ES je nutné považovat i činnost internetového vyhledávače *spočívající ve vyhledávání informací zveřejněných nebo umístěných na internetu třetími osobami, v jejich automatickém indexování, v jejich dočasném ukládání a konečně v jejich poskytování uživatelům internetu v určitém preferenčním pořadí*, samozřejmě za předpokladu, že součástí těchto informací jsou osobní údaje. SDEU dále dospěl k závěru, že provozovatel takového internetového vyhledávače by měl být kvalifikován jako správce ve smyslu Směrnice 95/46/ES.

2.4 Správce osobních údajů

Správcem osobních údajů je, dle čl. 4 odst. 7 GDPR, subjekt, který samostatně nebo kolektivně stanovuje účel a prostředky zpracování osobních údajů. Tímto subjektem může být zejména fyzická či právnická osoba, orgán veřejné moci nebo agentura. Definice tohoto pojmu je opět takřka doslovně přejata ze znění Směrnice 95/46/ES. Definice obsažená v ZOOÚ je oproti Směrnici 95/46/ES i GDPR méně konkrétní v tom smyslu, že neobsahuje demonstrativní výčet subjektů, kteří mohou být správci, na druhou stranu ale přímo zahrnuje dva z příznačných znaků pro správce osobních údajů, a to provádění zpracování osobních údajů a odpovědnost za toto zpracování.[111]

Analýze pojmu správce se věnovala WP29 v jednom ze svých stanovisek. Jako hlavní význam pojmu správce je zde označeno určení toho, kdo je odpovědný za

110 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 86-87.
111 Srov. § 4 písm. j) ZOOÚ.

dodržování pravidel pro ochranu osobních údajů a způsobu jak subjekty osobních údajů mohou uplatňovat svá práva. Osobou odpovědnou za dodržení pravidel upravujících zpracování osobních údajů je přitom právě správce.[112]

V GDPR, stejně jako ve Směrnici 95/46/ES, sice odpovědnost správce za zpracování osobních údajů není obsažena přímo v definici pojmu správce, nicméně je uvedena na několika jiných místech, a to v recitálu 74, v čl. 5 odst. 2 a čl. 24 GDPR. Důležité je, jak již bylo uvedeno v kapitole 1. této práce, že v novém pojetí odpovědnosti dle GDPR je výslovně zakotvena nejen odpovědnost správce za zpracování osobních údajů, ale i povinnost doložit soulad zpracování s tímto nařízením, což, dle názoru autorky, představuje jednu ze zásadních změn, které přineslo GDPR. Odpovědnost za zpracování lze rozdělit na veřejnoprávní a soukromoprávní. Veřejnoprávní odpovědnost plyne z každého ustanovení GDPR, které ukládá správci určitou povinnost s tím, že při jejím nesplnění hrozí správci uložení správní sankce. Soukromoprávní odpovědnost, tedy oprávnění subjektu údajů domáhat se svých práv garantovaných GDPR u soudu, je potom upravena v čl. 79 GDPR.[113]

Samotnou definici pojmu správce je možné rozdělit na tři hlavní prvky, a to prvek osobní („*fyzická nebo právnická osoba….“*), možnost mnohostranné kontroly („*sám nebo společně s jinými“*) a prvek odlišující správce od ostatních subjektů podílejících se na zpracování osobních údajů („*určuje účely a prostředky zpracování“*). Pod osobním aspektem si lze představit škálu subjektů, které mohou být v pozici správce. Vždy se přitom upřednostňuje, aby byla za správce považována společnost, nebo orgán, nikoliv určitý jedinec v rámci společnosti či orgánu. Možnost mnohostranné kontroly se dotýká situací, kdy při zpracování osobních údajů jako správce jedná více účastníků, kteří by si mezi sebou měli jednoznačně rozdělit úlohy při určování účelů a prostředků zpracování a odpovědnost. Možnost určit účely a prostředky zpracování pak vyplývá typicky z rozličných právních a/nebo skutkových okolností.[114]

Správcem může být osoba, která se sama rozhodne, že bude zpracovávat osobní údaje za účelem dosažení určitého cíle (např. za účelem oslovení zákazníků, za účelem ochrany svého majetku apod.) a určí prostředky zpracování. V některých případech ale může být správci uložena zákonem povinnost zpracování osobních údajů za určitým

112 WP29: Stanovisko č. 1/2010 *k pojmům „správce“ a „zpracovatel“* přijaté dne 16. února 2010.
113 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*, op. cit. s. 88 - 89.
114 WP29: Stanovisko č. 1/2010 *k pojmům „správce“ a „zpracovatel“* op. cit.

účelem. Účel a někdy i prostředky zpracování v tomto případě stanoví zákonodárce.[115] Jako příklad zpracování uloženého správci zákonem lze uvést zpracování osobních údajů v oblasti pracovněprávních vztahů, kde platí, že zaměstnavatelé jsou v řadě případů ze zákona povinni zpracovávat osobní údaje svých zaměstnanců, např. jsou povinni vést evidenci pracovní doby zaměstnance, účet jeho mzdy či evidenci údajů oznamovaných zdravotní pojišťovně.[116]

Na rozdíl od Směrnice 95/46/ES a ZOOÚ GDPR v čl. 26 vymezuje také institut společných správců, který se týká případů, kdy účely a prostředky zpracování určuje společně více správců. Z takového společenství pro správce plyne zejména povinnost vymezit si mezi sebou podíly na odpovědnosti a plnění povinností dle GDPR.

2.5 Zpracovatel osobních údajů

Definice zpracovatele obsažená v čl. 4 odst. 8 GDPR přejatá ze Směrnice 95/46/ES je poměrně stručná a zní následovně *„zpracovatelem" (se rozumí) fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce*.

Zpracovatel je tedy dalším ze subjektů, který se účastní zpracování osobních údajů. Na rozdíl od správce ale není jeho účast obligatorní, záleží totiž zpravidla jen na uvážení správce, zda zpracovatele využije. Správce se může rozhodnout, že na zpracovatele přenese část zpracování osobních údajů, které provádí, ale pokud se mu to bude zdát efektivní (zejména z hlediska hospodářského), může zpracovatele pověřit celým zpracováním. V některých, spíše výjimečných, případech je určitý subjekt za zpracovatele osobních údajů označen v právním předpise. Příkladem je § 18 odst. 3 zákona č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon), kde je výslovně uvedeno, že Koordinační středisko transplantací je zpracovatelem osobních údajů vedených v registrech vyčtených v tomto ustanovení ve smyslu ZOOÚ.[117]

V praxi se může stát, že nebude jednoduché stanovit, zda se v určitých případech bude jednat o správce nebo zpracovatel. Pro rozlišení těchto rolí při zpracování je třeba se předně zaměřit na to, kdo zejména určuje účel zpracování, protože jedině správce je

115 MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích. 1. vydání*, op. cit. s. 221.
116 NONNEMANN, F. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář. 1. vydání*, op. cit. s. 78.
117 NONNEMANN, F. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: Zákon o ochraně osobních údajů. Komentář. *1. vydání*, op. cit. s. 82 - 83.

subjektem, který je oprávněný rozhodnout o účelech zpracování. Zpracovatel „pouze" plní povinnosti, které mu stanoví GDPR a pokyny správce týkající se zpracování. Zpracovatel zpracovává osobní údaje *pro* správce (je pověřen správcem), což je klíčová část definice tohoto pojmu; zpracovatel tedy nemůže údaje, které mu za účelem zpracování správce předá, zpracovávat pro vlastní účely.[118] Pokud by zpracovatel překročil pověření dané správcem a získal úlohu při určování účelu zpracování nebo základních prostředků zpracování, vztah mezi ním a správcem by se z roviny správce - zpracovatel přesunul do roviny správce – správce, a stal by se společným správcem.[119]

Co se týče vztahu mezi správcem a zpracovatelem, tento je poměrně detailně upraven v čl. 28 GDPR. Oproti úpravě vztahu správce a zpracovatele obsažené ve Směrnici 95/46/ES či v ZOOÚ je ta v GDPR daleko širší. Toto ustanovení ukládá správci mj. povinnost zapojit do zpracování jen ty zpracovatele, kteří dostatečně zaručují zavedení technických a organizačních opatření splňujících požadavky GDPR pro zpracování či zpracovateli povinnost nezapojit do zpracování dalšího zpracovatele (tzv. řetězení zpracovatelů) bez předchozího souhlasu správce. Vztah mezi správcem a zpracovatelem se zpravidla bude řídit smlouvou o zpracování osobních údajů, byť GDPR nevylučuje, aby byl tento vztah upraven i jiným právním aktem dle práva EU nebo členských států. Požadavky na obsah smlouvy či jiného právního aktu, které musí být ze strany správce a zpracovatele vždy splněny, jsou stanoveny v čl. 28 odst. 3 GDPR. Co se týče formy, platí, že právní akt upravující vztah mezi správcem a zpracovatelem musí mít písemnou formu, přičemž za písemnou se považuje i elektronická forma.[120]

Od osoby zpracovatele je třeba odlišit osobu, která zpracovává osobní údaje z pověření správce nebo zpracovatele ve smyslu čl. 29 GDPR, i na ní se vztahuje povinnost zpracovávat osobní údaje pouze na základě pokynů správce s výjimkou, kdy má povinnost údaje zpracovávat dle práva EU nebo dle vnitrostátní právní úpravy. Takovými osobami typicky budou zaměstnanci správce či členové jeho statutárního orgánu.

118 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 89.
119 WP29: Stanovisko č. 1/2010 *k pojmům „správce" a „zpracovatel"* op. cit.
120 Čl. 28 odst. 9 GDPR.

2.6 Příjemce osobních údajů

Poslední pojem, který bude v rámci této kapitoly vymezen, je pojem příjemce osobních údajů. GDPR v čl. 4 odst. 9 jako příjemce označuje subjekty, kterým jsou osobní údaje poskytnuty, ať se jedná o třetí osobu ve smyslu čl. 4 odst. 10 nebo nikoliv[121].

Stejně jako v definici pojmu správce je i v definici tohoto pojmu dále obsažen výčet subjektů, kteří mohou být příjemcem. Jedná se o fyzickou nebo právnickou osobu, orgán veřejné moci, agenturu či jiný subjekt. Ve větě druhé čl. 4 odst. 9 je uvedeno, kdo se naopak za příjemce nepovažuje, jde o orgány veřejné moci, které mohou získávat osobní údaje v souvislosti se zvláštním šetřením dle práva členského státu.

Jak vyplývá z výše uvedeného, příjemcem může být např. i další správce (rozdílný od původního), zpracovatel, či subjekt údajů. Rozhodující pro označení subjektu jako příjemce je moment předání či zpřístupnění osobních údajů. Právě v tomto okamžiku může být subjekt označen za příjemce, jakmile by začal ze své vlastní vůle údaje dále zpracovávat, stal by se samostatným správcem osobních údajů a musel by plnit všechny povinnost vyplývající z právních předpisů na ochranu osobních údajů. Výlučně příjemcem tak může být subjekt jen po omezenou dobu.[122]

I definice tohoto pojmu nebyla s účinností GDPR prakticky vůbec změněna a byla skoro doslovně přejata ze Směrnice 95/46/ES. Žádný výrazný rozdíl, který by měnil pojetí pojmu příjemce, není ani ve srovnání se ZOOÚ.

121 Třetí stranou se ve smyslu čl. 4 odst. 10 GDPR rozumí subjekt odlišný od subjektu údajů, správce, zpracovatele či osoby přímo podléhající správci nebo zpracovateli oprávněné ke zpracování osobních údajů.

122 NONNEMANN, F. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář. 1. vydání*, op. cit. s. 92 - 93.

3 Zásady zpracování osobních údajů

Základní zásady zpracování osobních údajů obsažené v čl. 5 GDPR je možné označit jako základní pilíře, na kterých staví GDPR. Základními zásadami se řídí celé GDPR a všechna ustanovení GDPR musí být interpretována tak, aby byla s nimi v souladu. Zároveň také platí, že zásady zpracování uvedené v čl. 5 jsou přímo vynutitelné, tedy při jejich porušení hrozí správci osobních údajů uložení správní pokuty dle čl. 83 odst. 5 GDPR.[123] Zásady zpracování osobních údajů vyčtené v čl. 5 odst. 1 GDPR lze považovat za základní povinnosti správce, které musí při provádění zpracování osobních údajů splnit. V ZOOÚ ostatně byly jednotlivé zásady označeny jako povinnosti správce při zpracování osobních údajů. [124]

K základním zásadám zpracování osobních údajů se řadí zásada zákonnosti, korektnosti, transparentnosti, zásada účelového omezení, minimalizace údajů, přesnosti, omezení uložení, integrity a důvěrnosti. Všechny výše uvedené zásady budou blíže rozebrány níže v této kapitole. V této kapitole diplomové práce budou zároveň přiblíženy všechny právní důvody zpracování osobních údajů obsažené v čl. 6 GDPR, neboť jsou úzce spjaté se zásadou zákonnosti zpracování osobních údajů.

Zásady uvedené v čl. 5 GDPR ve velké míře vycházejí ze zásad pro kvalitu údajů uvedených v čl. 5 Úmluvy č. 108 a především pak v čl. 6 Směrnice 95/46/ES. V GDPR se oproti výše uvedeným dokumentům v čl. 5 odst. 2 výslovně objevuje nový prvek odpovědnosti za dodržení zásad zpracování osobních údajů a povinnosti doložit soulad s těmito zásadami, což spadá pod nové pojetí principu odpovědnosti správce dle GDPR analyzované v kapitole 1. této práce.

3.1 Zákonnost

Zásadu zákonnosti lze označit jako nejdůležitější zásadu zpracování osobních údajů. Tato zásada stanoví, že správce je oprávněn provádět zpracování osobních údajů jen tehdy, když tak činí na základě minimálně jednoho z právních důvodů vyčtených v čl. 6 odst. 1.

Pro naplnění zásady zákonnosti zpracování je nutné posoudit kombinaci tří aspektů nakládání s osobními údaji. Zaprvé je třeba určit účel, za kterým je zpracování prováděno, dále je nutné zajistit právní základ zpracování a určit okruh zpracovávaných

123 PATTYNOVÁ J. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobnic údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. op. cit. s. 60.
124 § 5 ZOOÚ.

osobních údajů přiměřený účelu a podložený právním základem. Všechny tři výše uvedené aspekty je zapotřebí vnímat jako vzájemně provázané natolik, že když např. dojde k rozšíření účelu zpracování osobních údajů, bude třeba přezkoumat, zda tomuto rozšíření stále odpovídá právní základ zpracování i okruh dotčených osobních údajů.[125]

3.2 Právní důvody zpracování osobních údajů

Existenci právního důvodu pro zpracování osobních údajů je možné považovat za základní předpoklad k tomu, aby zpracování mohlo být pokládáno za souladné s právními předpisy na ochranu osobních údajů. Pokud by u správce od počátku zpracování osobních údajů absentoval právní důvod pro zpracování, bude jím prováděné zpracování považováno jako protiprávní, a správce bude povinen provést výmaz osobních údajů v souladu s čl. 17 odst. 1 písm. d) GDPR. Stejnou povinnost bude mít správce, kterému odpadne dříve existující právní důvod pro zpracování osobních údajů, pokud se na něj nebude vztahovat některá z výjimek uvedených v čl. 17 odst. 3 GDPR.

Jak již bylo nastíněno výše, správce provádí zpracování osobních údajů za konkrétním účelem a právní důvod zpracování musí vždy pokrývat takový účel.[126]

Právními tituly, na jejichž základě mohou být osobní údaje dle GDPR zpracovány, jsou souhlas subjektu údajů se zpracováním jeho osobních údajů, plnění smlouvy, v níž jako smluvní strana figuruje subjekt údajů, plnění právní povinnosti správce, ochrana životně důležitých zájmů subjektu údajů či jiné fyzické osoby, plnění úkolu správcem, a to ve veřejném zájmu nebo při výkonu veřejné moci a ochrana oprávněných zájmů správce nebo třetí strany.[127]

V českém prostředí byl v důsledku striktní nebo spíše nepřesné transpozice Směrnice 95/46/ES často chápán jako základní titul pro zpracování osobních údajů souhlas subjektu údajů.[128] Vycházelo se přitom z teze, že zpracování osobních údajů vždy znamená zásah do soukromí fyzické osoby, proto by mělo být zpracování přípustné zejména za situace, kdy s tím dotčený jedinec souhlasí, a až sekundárně pokud

125 KASL, F. in POLČÁK, R. a kol. *Právo informačních* technologií. Praha: Wolters Kluwer ČR, 2018, s. 437 ISBN 978-80-7598-045-8.

126 ŽŮREK J. *Praktický průvodce GDPR*. 2017, op. cit. s. 67.

127 Čl. 6 odst. 1 GDPR.

128 Čl. 7 písm. Směrnice 95/46/ES mj. stanoví, že „*zpracování osobních údajů může být provedeno pouze pokud subjekt údajů nezpochybnitelně udělil souhlas; nebo….“* V § 5 odst. 2 ZOOÚ se pak tato zásada promítla tím způsobem, že je zde uvedeno následující: „*Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,….“* (následuje výčet dalších právních titulů)

existuje legitimní zájem jiného subjektu, který převyšuje právo jedince na ochranu soukromí.[129] S názorem, že souhlas se zpracováním osobních údajů je preferovaným právním důvodem zpracování osobních údajů, se ztotožňovali i další autoři.[130]

V GDPR jsou, vzhledem k formulaci čl. 6 odst. 1, jednotlivé právní důvody zpracování osobních údajů zjevně rovnocenné.

Lze souhlasit se závěrem, že s ohledem na zpřísnění požadavků kladených na souhlas subjektu údajů v GDPR by nyní správce měl nejdříve přemýšlet nad tím, jestli zpracování osobních údajů nemůže podložit jiným právním důvodem uvedeným v čl. 6 odst. 1 GDPR, a až v případě, kdy dospěje k závěru, že nelze provádět zpracování osobních údajů na základě žádného z těchto důvodů, přistoupí k vyžádání si souhlasu od subjektu údajů. [131] Získání souhlasu subjektu údajů se zpracováním jeho osobních údajů totiž bude pro správce v drtivé většině případů daleko obtížnější a nákladnější než snaha nalézt jiný právní důvod pro zpracování, zároveň také nelze přehlédnout riziko, že subjekt svůj souhlas může v souladu s čl. 7 odst. 3 kdykoliv odvolat.

3.2.1 Souhlas subjektu se zpracováním osobních údajů

Jako první je v seznamu právních titulů pro zpracování osobních údajů v čl. 6 odst. 1 GDPR uveden souhlas subjektu údajů. Souhlas je jako jediný z existujících právních důvodů pro zpracování osobních údajů výslovně uveden už v čl. 8 odst. 2. Listiny základních práv EU, který stanoví, že osobní údaje musí být zpracovány *na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem*.

Souhlas je jediným titulem pro zpracování osobních údajů, který předpokládá aktivní jednání subjektu osobních údajů, čímž se liší od ostatních důvodů zpracování. Souhlas bude mít své uplatnění v případech, kdy správci nebude svědčit jiný z právních důvodů zpracování uvedených v čl. 6 odst. 1. Použití souhlasu je ale podmíněno také tím, že správce bude provádět zpracování za legitimním účelem.[132]

129 NOVÁKOVÁ, L. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář. 1. vydání*. op. cit. s. 132 - 133.

130 Srov. MAŠTALKA, J. *Osobní údaje, právo a my*. 1. vydání, op. cit. s. 48.

131 Srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 124.

132 ŽŮREK J. *Praktický průvodce GDPR*, op. cit. s. 68 - 71.

V praxi často dochází k tomu, že správci a zpracovatelé požadují souhlas se zpracováním osobních údajů po subjektech údajů nadbytečně a neoprávněně. Typickým příkladem je sektor bankovních nebo telekomunikačních služeb, kdy jde o služby poskytované obvykle dle zákona nebo smlouvy, a tudíž i osobní údaje klientů poskytovatelů těchto služeb jsou zpracovávány z důvodu plnění zákona či smlouvy. Poskytovatelé takových služeb nicméně přesto po svých klientech často požadují udělení souhlasu se zpracováním jejich osobních údajů a na jeho poskytnutí vážou poskytování samotné služby navzdory tomu, že je takový postup v rozporu s GDPR.[133]

Skutečnost, že souhlas bývá v praxi často vyžadován opravdu nadbytečně, je posílena i faktem, že v běžném životě obvykle dochází ke zpracování osobních údajů na základě jiného titulu, typicky z důvodu plnění smlouvy uzavřené mezi správcem a subjektem údajů, z důvodu plnění zákonné povinnosti správce nebo ochrany oprávněného zájmu. Kromě toho, že postup správce, který vyžaduje od subjektu údajů souhlas, i když ke zpracování existuje reálně jiný právní důvod, je možné označit jako nadbytečný, lze tento považovat též za klamavý. Správce totiž v subjektu údajů vyvolá dojem, že prováděné zpracování je založeno na jeho projevu vůle, který je možné kdykoliv odvolat. Nicméně jestliže je správci údajů např. uložena zákonná povinnost zpracovávat osobní údaje subjektu, který odvolal svůj souhlas, správce ani po odvolání souhlasu zpracování osobních údajů neukončí (a ani jej ukončit nemůže, aniž by neporušil právní předpisy). Často tak subjekt údajů v podstatě ztrácí kontrolu nad svými osobními údaji, když jej správce mnohdy ani neinformuje o skutečnosti, že navzdory odvolání souhlasu nadále zpracovává jeho osobní údaje z důvodu plnění zákonných povinností.[134] Nesplnění informační povinnosti vůči subjektu údajů (nesprávné či klamavé informování o právním základu zpracování či vůbec o skutečnosti, že osobní údaje určitého subjektu jsou zpracovávány), lze přitom chápat jako porušení jedné ze základních zásad zpracování osobních údajů – zásady transparentnosti, za které může být správce dle GDPR sankcionován pokutou ve výši až 20.000.000 EUR (resp. 4 % ročního obratu).[135]

Co se týče získání souhlasu se zpracováním osobních údajů od subjektu, platí, že na výzvu k udělení souhlasu adresovanou subjektu údajů by se obecně měla vztahovat přísná pravidla, a to z toho důvodu, že se dotýká základních práv subjektu údajů a

133 Tisková zpráva ÚOOÚ ze dne 31. srpna 2018. *Sdělení předsedkyně Úřadu k vyžadování souhlasu*. Dostupné na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31695.

134 ÚOOÚ: Stanovisko č. 3/2014 *K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti.*

135 Čl. 83 odst. 5 písm. b) GDPR.

správce zamýšlí zahájit zpracování osobních údajů, které by bez udělení souhlasu ke zpracování nebylo v souladu s právem.[136]

To, že je zpracování osobních údajů prováděno na základě souhlasu subjektu údajů neznamená, že by správce nemusel v plném rozsahu dodržovat zásady uvedené v čl. 5 GDPR, včetně zásady účelového omezení a minimalizace údajů. I když je právním důvodem pro zpracování souhlas subjektu údajů, správce musí zpracovávat osobní údaje vždy jen v rozsahu nezbytném pro naplnění účelu, za kterým jsou zpracovávány.[137]

Pojem „souhlas“ je vymezen i v čl. 4 GDPR obsahujícím definice základních pojmů, se kterými toto nařízení operuje. Čl. 4 odst. 11 GDPR pojem souhlas subjektu údajů definuje jako *„svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“*

Aby byl souhlas platný, musí, v souladu se shora uvedenou definicí, zahrnovat 4 základní prvky, tedy musí být svobodný, konkrétní, informovaný a musí jít o jednoznačný projev vůle dát svolení ke zpracování svých osobních údajů. Jednotlivé prvky souhlasu blíže rozebírá i WP29 ve svém stanovisku a pokynech týkajících se problematiky souhlasu se zpracováním osobních údajů.

Aby mohl být souhlas se zpracováním osobních údajů označen jako svobodný, platí, že subjekt údajů musí mít možnost kontroly nad zpracováním jeho osobních údajů a možnost skutečné volby mezi přijetím či odmítnutím navrhovaných podmínek, aniž by tím byl poškozen. Jakmile subjekt údajů bude cítit tlak, který mu bude bránit svobodně projevit svoji vůli, nebo pokud neposkytnutí souhlasu s sebou přinese negativní následky pro subjekt údajů, souhlas nebude možné považovat jako platný.[138]

Souhlas je konkrétní, pokud je udělen pro jeden či více konkrétních účelů[139] a subjekt údajů má možnost volby ve vztahu ke každému jednotlivému účelu zpracování. Cílem požadavku konkrétnosti je zajištění kontroly uživatele a transparentnosti pro subjekt údajů.[140]

Požadavek, aby byl souhlas ke zpracování osobních údajů informovaný je v GDPR oproti předchozí právní úpravě posílen. Lze jej spojit se zásadou

136 WP29: Stanovisko č. 15/2011 *o definici souhlasu* přijaté dne 13. července 2011.
137 Tamtéž.
138 WP29: Stanovisko č. 15/2011 *o definici souhlasu*, op. cit.
139 Čl. 6 odst. 1 písm. a) GDPR.
140 WP29: *Pokyny pro souhlas podle nařízení 2016/679* přijaté dne 28. listopadu 2017, v revidovaném znění přijatém dne 10. dubna 2018.

transparentnosti, která je uvedena ve výčtu zásad zpracování osobních údajů v čl. 5 GDPR. K tomu, aby byl souhlas posouzen jako informovaný, je nutné splnit informační povinnost vůči subjektu údajů tak, aby si mohl zvolit, zda souhlas udělí nebo ne. Dle názoru WP29 musí správce poskytnout před udělením souhlasu subjektu údajů alespoň následující informace: totožnost správce, účel operace zpracování, pro kterou je požadován souhlas, typy údajů, které budou zpracovávány, upozornění na možnost souhlas odvolat, o hrozících rizicích předávání údajů z důvodu absence rozhodnutí o odpovídající ochraně a vhodných zárukách, případně o využití údajů pro automatizované rozhodování dle čl. 22 odst. 2 písm. c). Informace může správce předat ve formě písemné, ústní, ale třeba i v podobě videozprávy, v každém případě by měly být informace poskytnuty tak, aby byly snadno srozumitelné také pro průměrně znalé osoby, nikoliv jen pro odborníky.[141] V případě, že bude zpracování cílit na děti, správce by měl zajistit, aby byly informace poskytnuty tak, že budou pochopitelné i pro děti.[142]

Posledním ze čtyř základních předpokladů platnosti souhlasu se zpracováním osobních údajů je jednoznačný projev vůle. Souhlas musí být ze strany subjektu údajů poskytnut tak, aby bylo zřejmé, že šlo o jeho úmyslné aktivní jednání, jehož cílem je vyjádření souhlasu s daným zpracováním, tedy půjde o zjevné potvrzení, že subjekt se zpracováním souhlasí.[143] Souhlas subjektu údajů se zpracováním osobních údajů může mít formu písemného prohlášení, včetně takového, které bude učiněno elektronicky, či ústního prohlášení (zaznamenaného). Jako příklad platného udělení souhlasu si lze představit zaškrtnutí pole při návštěvě webové stránky, naopak mlčení, nečinnost nebo předem zaškrtnutá pole nemohou být považovány za souhlas ve smyslu GDPR.[144] Správce by měl vždy pamatovat na to, že souhlas musí v situacích, kdy je to nezbytné, získat ještě před tím, než zahájí samotné zpracování.[145] Tento závěr podporuje i formulace čl. 6 odst. 1 písm. a) GDPR, ze kterého plyne, že zpracování je zákonné, pokud *subjekt údajů udělil souhlas*. Z použití minulého času vyplývá, že souhlas musel existovat již před zahájením zpracováním.

Platnost souhlasu je dále podmíněna dodržením pravidel pro vyjádření souhlasu obsažených v čl. 7 GDPR, tyto do určité míry navazují na základní prvky platného souhlasu popsané výše. Předně je zde stanovena povinnost správce doložit udělení souhlasu subjektem ke zpracování jeho osobních údajů, což zahrnuje i doložení toho, že

141 Tamtéž.
142 Recitál 58 GDPR.
143 WP29: *Pokyny pro souhlas podle nařízení 2016/679*, op. cit.
144 Recitál 32 GDPR.
145 WP29: Stanovisko č. 15/2011 *o definici souhlasu*, op. cit.

správce dle GDPR řádně informoval subjekt údajů o všech skutečnostech a že souhlas splňuje veškerá kritéria stanovená GDPR. Tato povinnost bude trvat stejnou dobu, jako samotné zpracování, pro které byl souhlas udělen. Konkrétní doba, po kterou by měl být platný souhlas, v GDPR uvedena není; vždy bude nutné přihlížet k rozsahu souhlasu a očekávání subjektů údajů, přičemž jakmile dojde k výraznější změně zpracování, stávající souhlas již nebude platný. Způsob, jakým má správce prokázat udělení souhlasu v GDPR přesně stanoven není.[146] Aby však byl správce schopen prokázat udělení souhlasu, jako vhodnější se jeví písemná forma souhlasu, v případě provozovatelů různých webových stránek budou souhlasy obvykle zaznamenávány elektronicky (pomocí logů apod.).[147]

Dále je v čl. 7 GDPR obsažen požadavek na odlišitelnost souhlasu, souhlas tedy musí být jednoznačně odlišitelný od jiných skutečností, pokud je vyjádřen v písemném prohlášení týkajícím se také těchto skutečností. Pokud tedy bude souhlas např. součástí smlouvy, souhlas by měl být v rámci ní jasně odlišen od ostatního obsahu, popřípadě by měl být obsažen v samostatném dokumentu.[148]

Další z požadavků obsažených v čl. 7 GDPR jsou požadavky, aby byl souhlas poskytnutý ve srozumitelném a snadno přístupném znění.[149]

Poslední z důležitých aspektů souhlasu obsažený v čl. 7 GDPR je právo subjektu osobních údajů svůj souhlas kdykoliv odvolat. Právě tento prvek znamená určitou nestabilitu zpracování; pro správce jistě není žádoucí, když se ocitne v situaci, kdy subjekt náhle odvolá souhlas se zpracováním osobních údajů pro určité účely, a správce tak musí řešit ukončení zpracování osobních údajů jednoho konkrétního subjektu, a jeho osobní údaje vymazat (samozřejmě pokud mu nesvědčí jiný právní důvod pro zpracování). Čl. 7 odst. 3 GDPR výslovně stanoví, že odvolání souhlasu se zpracováním osobních údajů působí jen do budoucna, nikoliv retroaktivně, tedy neohrozí zákonnost zpracování prováděného před odvoláním souhlasu. Dále též platí, že pro subjekt údajů musí být odvolání souhlasu stejně snadné jako jeho poskytnutí. V ideálním případě, by subjekty údajů měly mít možnost souhlas odvolat úplně stejnými prostředky, jakými jej udělily (např. jedinec udělí správci souhlas se zpracováním osobních údajů telefonicky, správce by přitom měl také sdělit číslo, prostřednictvím kterého může být souhlas odvolán). Odvolání souhlasu nesmí přivodit subjektu údajů žádnou újmu, pokud by

146 WP29: *Pokyny pro souhlas podle nařízení 2016/679*, op. cit.
147 Srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 125.
148 WP29: *Pokyny pro souhlas podle nařízení 2016/679*, op. cit.
149 Tamtéž.

např. správce sankcionoval odvolání souhlasu pokutou, nebyl by takový souhlas od počátku platný, protože by nemohl být považován za svobodný.[150]

Souhlasy ke zpracování osobních údajů, které byly uděleny před účinností GDPR bude možné nadále považovat jako platné právní tituly pro zpracování osobních údajů, a správce si nebude muset vyžádat od subjektu nový souhlas jen v případě, že způsob udělení souhlasu splňuje podmínky, které na souhlas klade GDPR.[151] Pokud souhlas nebude splňovat požadavky GDPR, bude nutné si vyžádat nový souhlas od subjektu údajů, nalézt jiný právní důvod, který by ospravedlňoval pokračování v daném zpracování osobních údajů, anebo zpracování ukončit.

Vzhledem k tomu, že souhlas ke zpracování osobních údajů je bezpochyby právním jednáním, musí, pokud se bude řídit českým právním řádem, splňovat též náležitosti právního jednání zakotvené v § 545 a násl. zákona č. 89/2012 Sb., občanského zákoníku („OZ“). Použije se logicky také právní úprava o svéprávnosti a zákonném zastoupení obsažená v OZ, proto budou v některých případech za děti udělovat souhlas se zpracováním osobních údajů jejich zákonní zástupci. Souhlas rodičů by měl být přitom dán vždy, když dle § 31 OZ, s přihlédnutím k rozumové a volní vyspělosti, nebudou děti schopny správně vyhodnotit povahu a důsledky souhlasu, včetně všech aspektů souvisejících se zpracováním jejich osobních údajů, tedy nebudou samy způsobilé v dané věci právně jednat, a souhlas udělit.[152] Pakliže by dítě udělilo souhlas se zpracováním jeho osobních údajů, aniž by bylo způsobilé v daném konkrétním případě samo právně jednat (např. účel zpracování by byl příliš složitý na to, aby mu porozumělo), bylo by takové jeho jednání posouzeno v souladu s § 581 OZ jako neplatné. Většina odborné veřejnosti se pak přiklání ke stanovisku, že se jedná o neplatnost absolutní, jelikož jde o jednání, které je ve zřejmém rozporu se smyslem a účelem zákona.[153]

Zvláštní pravidla, co se týče souhlasu dětí se zpracováním jejich osobních údajů, jsou stanovena pro souhlas související se službami informační společnosti, a to v čl. 8 GDPR. Jedná se o určitý posun oproti Směrnici 95/46/ES, ve které nebyla stanovena vůbec žádná zvláštní pravidla dotýkající se zpracování osobních údajů dětí.

---

150 Information Commissioner's Office. *Consultation: GDPR consent guidance*. Dostupné na https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

151 Recitál 171 GDPR.

152 Srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 125.

153 DOBROVOLNÁ, E. in LAVICKÝ, P. *a kol.: Občanský zákoník I. Obecná část (§ 1−654). Komentář*. 1. vydání, Praha: C. H. Beck, 2014, s. 2093 – 2094, ISBN 978-80-7400-529-9.

Čl. 8 GDPR navazuje na recitál 38 GDPR, který stanoví, že dětem má být zaručena zvláštní ochrana osobních údajů, a to z důvodu jejich nezkušenosti, kdy jsou si často méně vědomy rizik, důsledků a svých práv v souvislosti se zpracováním osobních údajů. Zvláštní ochrana dětí by se, dle recitálu 38 GDPR, měla aplikovat zejména při používání jejich osobních údajů pro marketingové účely, pro účely vytváření osobnostních či uživatelských profilů a shromažďování osobních údajů dětí při využívání služeb nabízených přímo dětem.

Pojem služba informační společnosti, se kterým je pracováno v čl. 8 GDPR, je definována ve Směrnici Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti jako *„každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.“*[154] Tato definice se použije pro účely GDPR na základě odkazu na výše uvedenou definici obsaženého v čl. 4 odst. 25 GDPR.

Bude-li využit jako právní titul pro zpracování osobních údajů dítěte v souvislosti s nabídkou služeb informační společnosti (ve smyslu výše uvedené definice) přímo dítěti, je nutné, kromě podmínek pro vyjádření souhlasu dle čl. 7 GDPR, splnit zvláštní požadavek, kterým je minimální věk dítěte 16 let. U dětí mladších 16 let musí být takový souhlas vyjádřen nebo schválen osobou vykonávající rodičovskou zodpovědnost k dítěti.[155] V opačném případě by se jednalo o nezákonné zpracování osobních údajů.

Zajímavou otázkou je, jak bude možné v těchto případech v praxi prokázat, že souhlas udělila osoba, která dosáhla požadovaného věku, nebo že byl tento souhlas vyjádřen nebo schválen osobou vykonávající rodičovskou zodpovědnost. V čl. 8 odst. 2 GDPR je stanoveno, že správce má povinnost vyvinout přiměřené úsilí s ohledem na dostupnou technologii za účelem ověření, že souhlas byl vyjádřen nebo schválen osobou vykonávající rodičovskou zodpovědnost k dítěti; povinnost vyvinout přiměřené úsilí k ověření věku dítěte udělujícího souhlas sice není v čl. 8 GDPR výslovně uvedena, ale logicky je také třeba ji brát v potaz, jelikož nedostatečný věk dítěte udělujícího samostatně souhlas by znamenal protiprávnost prováděného zpracování.[156]

154 Čl. 1 odst. 1 písm. b) Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti.

155 Čl. 8 odst. 1 GDPR.

156 WP29: *Pokyny pro souhlas podle nařízení 2016/679*, op. cit.

Správce bude muset důkladně zvážit zavedení mechanismů, pomocí kterých v případech, kdy to bude nutné, ověří věk či skutečnost, že jde o osobou vykonávající rodičovskou zodpovědnost k dítěti. Takový mechanismus by samozřejmě měl co nejspolehlivěji vést k opravdovému zjištění požadovaných skutečností, zároveň ale nesmí příliš zasahovat do práv dotčených jedinců, zejména by neměl vést k nadměrnému zpracování osobních údajů, což může být v praxi poněkud problematické. Méně invazivní způsoby ověření jako je např. prohlášení fyzické osoby o svém věku při vstupu na webovou stránku, nebo potvrzení věku zadáním e-mailové adresy rodiče nelze považovat za příliš efektivní ve vztahu k dosažení účelu a více invazivní formy zase mohou vést mj. ke ztížení přístupu ke službě, nepřijatelné míře profilování či dalším nepřijatelným zásahům do práv dotčených jedinců jako je nadměrné shromažďování osobních údajů o nich v rámci provádění ověření.[157] Lze souhlasit s myšlenkou, že ne vždy bude nutné nejdříve ověřit věk dítěte a poté případně ověřit, zda osoba vykonávající rodičovskou zodpovědnost k dítěti vyjádřila nebo schválila souhlas a zda jde skutečně o k tomu oprávněnou osobu. V případě služeb informační společnosti, které se ze své podstaty zaměřují výhradně na malé děti (mladší 13 let) lze automaticky předpokládat, že souhlas osob s rodičovskou zodpovědností bude třeba vždy.[158]

V každém případě je problematika týkající se ověřování věku a souhlasu osoby vykonávající rodičovskou zodpovědnost ze shora uvedených důvodů velmi komplikovaná a pro správce ne úplně jasná, a bylo by na místě, aby se zejména Sbor k této otázce vyjádřil, a alespoň rámcově stanovil, v jakých konkrétních případech bude či nebude nutné uvedené skutečnosti ověřovat a jaké metody ověřování budou s ohledem na hrozící zásah do práv jedinců přijatelné.[159]

Jak již bylo naznačeno v kapitole první této práce, věková hranice 16 let nemusí platit plošně na celém území EU, GDPR totiž umožňuje, aby ji členské státy stanovily i jako nižší. V rámci Evropského digitálního trhu tak nebude existovat jednotná věková hranice, při jejímž dosažení budou děti oprávněny samy udělovat souhlas v souvislosti se službami informační společnosti, což není příliš žádoucí. Minimální věk pro udělení souhlasu dítěte v souvislosti se službami informační společnosti ale nesmí být nižší než 13 let. Česká republika možnosti upravit věkovou hranici pro souhlas dítěte

157 KASL, F. in POLČÁK, R. a kol. *Právo informačních* technologií. op. cit. s. 439-440.

158 MACENAITE M., KOSTA E. *Consent for processing children's personal data in the EU: following in US footsteps?* Information & Communications Technology Law, 26:2, s. 146 – 197, dostupné na https://doi.org/10.1080/13600834.2017.1321096.

159 Tamtéž.

v souvislosti se službami informační společnosti na vnitrostátní úrovni využila, s největší pravděpodobností bude stanovena věková hranice 15 let[160], která je považována za přiměřenější.[161]

Závěrem je k otázce udělování souhlasu ke zpracování osobních údajů dětmi nutné znovu zdůraznit, že věková hranice pro udělení souhlasu dětmi je v GDPR stanovena výlučně pro souhlas v souvislosti se službami informační společnosti. Ani ZOOÚ problematiku souhlasu dítěte se zpracováním osobních údajů nijak blíže neřeší, v ostatních případech souhlasů dětí se tedy na našem území budou aplikovat obecné podmínky vztahující se na souhlas se zpracováním osobních údajů dle GDPR a pravidla o jednání nezletilých obsažená v OZ.

Co se týče souhlasu jakožto právního důvodu pro zpracování osobních údajů v oblasti pracovněprávních vztahů, je nutné předně zmínit, že v této oblasti by měl být využíván jen výjimečně. I v pracovněprávních vztazích platí, že drtivá většina zpracování osobních údajů zaměstnanců zaměstnavatelem je prováděna na základě jiného právního důvodu (plnění právních povinností, plnění smlouvy, ochrana oprávněných zájmů), proto je vyžadování souhlasu zaměstnavatelem zpravidla nadbytečné.

Je navíc obecně považováno za problematické, aby zaměstnavatel zpracovával osobní údaje svých současných nebo budoucích zaměstnanců na základě souhlasu, jelikož je zde velká míra předpokladu absence prvku svobody. Mezi zaměstnavatelem a zaměstnancem existuje vztah závislosti a těžko si lze představit, že by zaměstnanec jakožto subjekt osobních údajů odmítnul udělit zaměstnavateli jako správci souhlas se zpracováním svých osobních údajů, aniž by pociťoval tlak či strach z nepříznivých následků.[162] Jedním z případů, kdy si lze představit využití souhlasu jako platného právního důvodu pro zpracování osobních údajů zaměstnanců zaměstnavatelem, je nakládání s fotografiemi zaměstnanců ze společenské události pořádané zaměstnavatelem, a to tím způsobem, že budou zveřejněny na profilu zaměstnavatele na sociální síti. Zaměstnavatel chce tyto fotografie na sociální síť umístit za účelem propagace společnosti, v dané situaci mu ale nesvědčí žádný z právních titulů uvedených v čl. 6 odst. 1 písm. b) – f), měl by tedy všechny zaměstnance, kteří budou na předmětných fotografiích, požádat o udělení souhlasu před tím, než fotografie

160 § 7 vládního návrhu ZZOÚ, sněmovní tisk 138/0, dostupné na http://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=138&CT1=0.

161 důvodová zpráva k vládnímu návrhu ZOOÚ, zvláštní část, sněmovní tisk 138/0, dostupné na http://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=138&CT1=0.

162 WP29: Stanovisko č. 2/2017 *ke zpracování údajů na pracovišti* přijaté dne 8. června 2017.

zveřejní. [163] V daném případě nelze předpokládat, že by rozhodování zaměstnance, zda souhlas se zveřejněním fotografie udělit, nebo ne, ovlivňoval vztah závislosti vůči zaměstnavateli, nebo že by dokonce zaměstnanci měla hrozit újma, pokud by souhlas neudělil, bylo by proto možné souhlas považovat za svobodný a pokud by splňoval i ostatní náležitosti souhlasu, tak také za platný.

3.2.2 Plnění smlouvy

Zpracování osobních údajů bude zákonné také tehdy, pokud jej bude správce činit z důvodu plnění již uzavřené smlouvy, jejíž smluvní stranou je subjekt údajů, nebo z důvodu, že je takové zpracování nezbytné k uzavření smlouvy se subjektem údajů (má-li subjekt údajů úmysl uzavřít smlouvu).[164]

Pod tento právní důvod lze tedy podřadit jednak zpracování osobních údajů, které správce činí, aby splnil svoje existující smluvní závazky, ale také zpracování prováděné v rámci jednání směřujícího k uzavření smlouvy (např. fyzická osoba s úmyslem požádat o hypoteční úvěr zašle bance vyplněný formuláře pro žádost o hypoteční úvěr, banka potom bude zpracovávat tyto údaje za účelem učinění opatření před uzavřením smlouvy, tedy bude vyhodnocovat, jestli hypoteční úvěr dané osobě poskytne, nebo ne). Správce osobních údajů by měl vždy dbát na to, aby v souladu se zásadou minimalizace údajů zpracovával vždy jen údaje, které budou nezbytné ve vztahu k předmětu smlouvy.

Příkladem, kdy bude zpracovávat osobní údaje z důvodu plnění smlouvy zaměstnavatel, je zpracování osobních údajů uchazečů o zaměstnání, kteří projevili zájem o uzavření pracovní smlouvy tím, že se přihlásili do výběrového řízení. V souladu s § 30 zákoníku práce by měl zaměstnavatel v rámci jednání před vznikem pracovního poměru vyžadovat od uchazečů pouze údaje bezprostředně související s uzavřením pracovní smlouvy. Spojení údaje bezprostředně související s uzavřením pracovní smlouvy je třeba vykládat tak, že jde o všechny údaje, *které jsou nutné ke svobodnému a vážnému rozhodnutí zaměstnavatele o tom, že s konkrétním zaměstnancem uzavře pracovní poměr"*.[165]

163 FOŘT F., PATTYNOVÁ J. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobníc údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. op. cit. s. 103.

164 Čl. 6 odst. 1 písm. b).

165 MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích. 1. vydání*, op. cit. s. 377.

Obecně by údaje, které zaměstnavatel získá o uchazečích během výběrového řízení, měly být vymazány, jakmile bude zjevné, že určité fyzické osobě nebude zaměstnání nabídnuto, nebo že dotčená fyzická osoba nepřijme nabídku zaměstnání.[166]

Na druhou stranu se objevuje i názor, že údaje, které zaměstnavatel získá o uchazečích během výběrového řízení, by si mohl legitimně ponechat (byť v takové podobě, že budou eliminovány nadbytečné údaje) z důvodu ochrany oprávněných zájmů pro případ, že by došlo k soudnímu sporu, v rámci kterého by se posuzovalo, zda zaměstnavatel ve výběrovém řízení nepostupoval diskriminačně, a zaměstnavatel by musel svůj postup konkrétně prokazovat. V takovém případě by doba uchování odpovídala promlčecí době.[167] Zaměstnavatel by samozřejmě musel uchazeče informovat o skutečnosti, že jeho osobní údaje budou zpracovávány i po skončení výběrového řízení z důvodu ochrany oprávněných zájmů zaměstnavatele jako správce.

Za trvání pracovního poměru samozřejmě zaměstnavatel také zpracovává některé osobní údaje zaměstnance z důvodu plnění pracovní smlouvy, kterou mezi sebou tyto dvě strany uzavřely. Takto mohou být zpracovávány např. osobní údaje spojené s výplatou mzdy, případných mimořádných odměn, či osobní údaje zpracovávané v souvislosti s poskytováním benefitů, ke kterému se zaměstnavatel zavázal v pracovní smlouvě (zpracování osobních údajů v souvislosti s poskytováním stravenek, poskytování příspěvků na penzijní připojištění, poskytování příspěvků na dopravu apod.).

3.2.3 Plnění právní povinnosti

Dalším legitimním důvodem pro zpracování osobních údajů může být plnění právní povinnosti, která se vztahuje na správce.[168] Právní předpisy přitom předpokládají, že aby správce splnil uloženou povinnost, bude muset provádět zpracování osobních údajů. Nutnost provádět zpracování osobních údajů bude v právních předpisech buď explicitně uvedena, nebo z nich bude plynout implicitně.

GDPR v čl. 6 odst. 3 písm. a) a b) dále specifikuje, že právní povinnost, která bude základem pro zpracování osobních údajů, musí být stanovena buď právem EU, nebo právem členského státu vztahujícího se na správce. Nikdy tedy nepůjde o

166 Rada Evropy, *doporučení Výboru ministrů Rady Evropy členským státům č. CM/Rec (2015) ohledně zpracování osobních údajů v souvislosti se zaměstnáním*, odstavec 13.2. Dostupné na https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a).

167 MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích. 1. vydání*, op. cit. s. 377.

168 Čl. 6 odst. 1 písm. c) GDPR.

povinnost, která by plynula z práva třetích zemí. V rámci České republiky budou pro správce základem zpracování povinnosti vyplývající buď z práva EU, nebo ze zákona.

Ustanovení právních předpisů, která jsou základem pro zpracování osobních údajů, často stanoví konkrétní účel zpracování osobních údajů správcem, dále mohou také označit kategorie osobních údajů, které budou zpracovány, dotčené subjekty údajů, subjekty, kterým mohou být osobní údaje poskytnuty, jakož i další podmínky, jejichž naplnění zajistí zákonnost a spravedlivost zpracování.[169]

Plnění právních povinností bude běžným důvodem pro zpracování osobních údajů zaměstnanců zaměstnavatelem. Právní povinnosti, k jejichž splnění je nutné zpracovávat osobní údaje, pro zaměstnavatele plynou zejména ze zákoníku práce, předpisů v oblasti práva sociálního zabezpečení či daňových předpisů. Souhrnně lze oblast zpracování osobních údajů zaměstnanců, které zaměstnavateli ukládají výše uvedené právní předpisy stanovující do určité míry i podmínky zpracování, označit jako zpracování osobních údajů pro účely vedení personální a mzdové agendy.[170]

Přímo v zákoníku práce je zaměstnavateli stanovena mj. povinnost vést evidenci pracovní doby jednotlivých zaměstnanců dle § 96, nebo povinnost vést v souladu s § 105 knihu úrazů obsahující evidenci všech úrazů zaměstnanců. Zaměstnavatel má, v souladu s § 312 odst. 1, právo vést osobní spis zaměstnance. V případě, že se zaměstnavatel rozhodne tohoto oprávnění využít, musí dodržet podmínky pro vedení osobního spisu stanovené dále v § 312. Jde o povinnost uchovávat v osobním spisu jen písemnosti nezbytné pro výkon práce v základním pracovněprávním vztahu, v zákoně není stanoven konkrétní výčet písemnosti, které může osobní spis zaměstnance obsahovat, lze však dovodit, že zaměstnavatel je oprávněn v rámci osobního spisu uchovávat např. osobní dotazník, profesní životopis, doklady o dosaženém vzdělání, přehled o odborné praxi, potvrzení o zaměstnání od předchozího zaměstnavatele či pracovní smlouvu[171]. Zaměstnavatel je též povinen respektovat okruh subjektů, které mají dle § 312 zákoníku práce právo nahlížet do osobních spisů zaměstnanců.

Zákoník práce ukládá zaměstnavateli povinnost zpracovat vymezený okruh osobních údajů zaměstnance také v souvislosti s vydáním potvrzení o zaměstnání dle § 313 zákoníku práce a pracovního posudku podle § 314 zákoníku práce. Potvrzení o zaměstnání je zaměstnavatel povinen vydat při skončení pracovního poměru, a to vždy

169 Čl. 6 odst. 3 GDPR.
170 MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích. 1. vydání*, op. cit. s. 174.
171 JANEČKOVÁ E., BARTÍK V. *Osobní spis zaměstnance jako zpracování osobních údajů,* Práce a mzda 2009/7.

zaměstnanci, nikoliv např. novému zaměstnavateli. Povinnost vydat potvrzení o zaměstnání je zaměstnavatel povinen splnit v souvislosti s ukončením pracovního poměru, nejpozději by proto tuto povinnost měl splnit v den, kdy pracovní poměr skončí. Osobní údaje, které má a smí potvrzení o zaměstnání obsahovat, jsou uvedeny v § 313 odst. 1 písm. a) – f) zákoníku práce. Teoreticky se zaměstnavatel se zaměstnancem mohou dohodnout i na tom, že v potvrzení o zaměstnání budou uvedeny i některé skutečnosti nad rámec těch uvedených v § 313 odst. 1 zákoníku práce.[172]

Na žádost zaměstnance je zaměstnavatel povinen vydat zaměstnanci posudek o pracovní činnosti (pracovní posudek), a to do 15 dnů ode dne podání žádosti zaměstnancem, zároveň ale zaměstnavatel není povinen tuto svoji povinnost splnit dříve než 2 měsíce před skončením pracovního poměru. Obsahem pracovního posudku jsou údaje o hodnocení práce zaměstnance, jeho kvalifikace a schopností, ale i další skutečnosti vztahující se k výkonu práce. Pracovní posudek tak může obsahovat i hodnocení vztahu zaměstnance k vykonávané práci, ke spolupracovníkům, ale také hodnocení vlastností zaměstnance, které mají bezprostřední vliv na výkon práce.[173]

Dalším příkladem zákonem uložené povinnosti zpracovávat osobní údaje zaměstnanců v souvislosti s vedením personální a mzdové agendy jsou povinnosti zaměstnavatele vést evidenci o zaměstnancích pro účely důchodového pojištění a vést evidenční listy důchodového pojištění zaměstnanců stanovené v § 37 a v § 38 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, v platném znění. V § 37 odst. 1 a v § 38 odst. 4 zákona uvedeného v předchozí větě je uveden výčet osobních údajů zaměstnanců, které mají zaměstnavatelé za účelem splnění této zákonné povinnosti zpracovat (např. jméno, příjmení, datum narození, bydliště, rodné číslo zaměstnance, druh výdělečné činnosti). § 35a odst. 4 téhož zákona dokonce určuje, jak dlouho má zaměstnavatel uchovávat evidenční listy důchodového pojištění (zpravidla 3 kalendářní roky po roce, kdy byly vyhotoveny), ale např. i mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění (30 či 10 kalendářních roků následujících po roce, kterého se týkají).

Jako další ze zákonných povinností vztahujících se na zaměstnance, která je základem pro zpracování osobních údajů zaměstnanců, lze uvést oznamovací povinnost zaměstnavatele vůči zdravotní pojišťovně zaměstnance dle § 10 zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů,

172 PUTNA, M. in BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář. 2. vydání*. Praha: C. H. Beck, 2015. s. 1229 - 1230. ISBN 978-80-7400-290-8.

173 Tamtéž s. 1233 – 1234.

v platném znění. Zákon č. 187/2006 Sb., o nemocenském pojištění, v platném znění, pak v § 95 ukládá zaměstnavateli povinnost vést evidenci o zaměstnancích účastných nemocenského pojištění.

V neposlední řadě se na zaměstnavatele vztahuje také povinnost vést pro zaměstnance (jakožto poplatníky daně z příjmů) mzdové listy, rekapitulaci o sražených zálohách a dani srážené podle zvláštní sazby daně za každý kalendářní měsíc i za celé zdaňovací období dle § 38j zákona č. 586/1992 Sb., o daních z příjmů, v platném znění. Mzdové listy přitom dle zákona musí obsahovat mj. identifikační údaje zaměstnance (včetně rodného čísla), identifikační údaje osoby, na kterou zaměstnanec uplatňuje slevu na dani či daňové zvýhodnění (typicky manžel/ka, dítě), den nástupu do zaměstnání, úhrn zúčtovaných mezd za každý kalendářní měsíc.

3.2.4 Ochrana životně důležitých zájmů

Zpracování osobních údajů bude zákonné i tehdy, když jej bude správce činit z důvodu nezbytnosti pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.[174] Tento právní titul pro zpracování osobních údajů by měl být ale legitimní jen v případech, kdy zpracování zjevně nemůže být založeno na jiném právním důvodu.[175]

Příkladem, kdy bude zpracování založeno na ochraně životně důležitého zájmu, může být zpracování osobních údajů oběti nehody, která není schopná udělit souhlas, za účelem poskytnutí lékařské péče ze strany poskytovatele zdravotní péče.

Oproti Směrnici 95/46/ES a ZOOÚ je možné zpracovávat osobní údaje na základě tohoto titulu i v případě, kdy se nejedná o životně důležitý zájem přímo subjektu údajů, ale i jiného jedince.[176] ZOOÚ dokonce, nad rámec Směrnice 95/46/ES, stanovil správci povinnost získat dodatečně souhlas subjektu údajů v případě, že byly jeho osobní údaje zpracovány z důvodu ochrany jeho životně důležitých zájmů.[177] Tato povinnost správce po účinnosti GDPR odpadá.

174 Čl. 6 odst. 1 písm. d) a recitál 46 GDPR.
175 Recitál 46 GDPR.
176 Srov. čl. 7 písm. d) Směrnice 95/46/ES a § 5 odst. 2 písm. c) ZOOÚ.
177 § 5 odst. 2 písm. c) ZOOÚ.

3.2.5 Plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci

K právním důvodům pro zpracování osobních údajů dle GDPR se řadí i plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.[178] Tento právní důvod se dotýká především zpracování osobních údajů prováděného orgány veřejné moci při výkonu jejich pravomocí; může se vztahovat ale i na osoby soukromého práva, které jsou pověřeny výkonem veřejné moci.

Právě tento právní titul, spolu s plněním právních povinností, bude téměř vždy základem pro zpracování osobních údajů prováděné orgány veřejné moci. Dle některých autorů rozdíl mezi dvěma výše uvedenými právními tituly tkví zejména ve formulaci ustanovení právního předpisu, který zmocňuje daného správce (orgán veřejné moci) ke zpracování osobních údajů. Pokud je právním předpisem stanoven konkrétní příkaz a správce nemá na výběr, zda učiní, co takový příkaz stanoví, nebo nikoliv, bude právním titulem plnění právní povinnosti. Naopak jestliže právní předpis dává správci úkol ve veřejném zájmu a pro jeho naplnění je nutné zpracovávat osobní údaje, bude právním titulem plnění úkolu ve veřejném zájmu. V tomto případě správce nemá zpracováním osobních údajů plnit konkrétní povinnost, správce je naopak oprávněn si v určitých případech v rámci svojí působnosti stanovit, jakým způsobem bude plnit úkol ve veřejném zájmu. Pakliže bude třeba za účelem splnění úkolu zvoleným způsobem zpracovávat osobní údaje, bude tak správce činit na základě důvodu plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci.[179]

Tento právní důvod pro zpracování osobních údajů byl obsažen i ve Směrnici 95/46/ES.[180] Ve výčtu právních titulů pro zpracování v § 5 odst. 2 ZOOÚ však chyběl, orgány veřejné moci proto do účinnosti GDPR při výkonu veřejné moci zpracovávaly osobní údaje hlavně na základě titulu plnění právních povinností.

Závěrem je k tomuto právnímu důvodu pro zpracování osobních údajů vhodné uvést, že je jedním ze dvou právních důvodů, kdy je subjekt údajů oprávněn vznést námitku proti zpracování osobních údajů dle čl. 21 odst. 1 GDPR. Druhým takovým právním důvodem je ochrana oprávněných zájmů správce nebo třetí strany.

178 Čl. 6 odst. 1 písm. e) GDPR.
179 Srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 130.
180 Čl. 7 písm. e) Směrnice 95/46/ES.

3.2.6 Oprávněný zájem správce nebo třetí strany

Posledním právním důvodem pro zpracování osobních údajů uvedeným v čl. 6 odst. 1 GDPR je oprávněný zájem příslušného správce nebo třetí strany. Jedná se o právní důvod, který je možné označit jako „sběrný“, a to z toho důvodu, že pod něj lze zahrnout různá zpracování, která nemohou spadat pod jiné právní důvody umožňující zpracování bez souhlasu subjektu osobních údajů, ale je spravedlivé, aby správce mohl v určitých případech osobní údaje zpracovávat, aniž by se musel spoléhat na poněkud nejistý souhlas subjektu údajů.[181] Tento právní důvod by se nikdy neměl vztahovat na zpracování osobních údajů prováděné orgány veřejné moci při plnění jejich úkolů, neboť právní základ pro zpracování osobních údajů orgány veřejné moci by měl být upraven v právním předpise.[182]

Zpracování na základě tohoto právního důvodu by nebylo zákonné, pokud by před oprávněnými zájmy správce nebo třetí strany měly přednost zájmy nebo základní práva a svobody subjektu údajů. Zohledněno přitom má být přiměřené očekávání subjektu údajů dle vztahu mezi ním a správcem, tedy subjekt údajů by měl mít v daném okamžiku a kontextu důvod očekávat, že může dojít ke zpracování jeho osobních údajů z důvodu ochrany oprávněných zájmů správce.[183]

Před tím, než zahájí zpracování osobních údajů na základě tohoto právního titulu, musí správce poměřit svoje oprávněné zájmy se zájmy nebo základními právy a svobodami subjektu údajů, aby zjistil, zda v daném případě tyto zájmy či základní práva a svobody subjektu údajů nepřeváží jeho oprávněné zájmy. V zásadě by tedy měl správce provést test proporcionality.[184] Ke zpracování osobních údajů z důvodů ochrany oprávněných zájmů by tedy mělo dojít jen, pokud půjde o zájem skutečně legitimní, zpracování osobních údajů bude nezbytné k ochraně zájmu a nad takovým oprávněným zájmem nepřeváží jiné zájmy nebo základní práva a svobody subjektu údajů.

Prvním krokem při posuzování, zda bude správce oprávněn zpracovávat osobní údaje z důvodu ochrany oprávněných zájmů, je vymezení oprávněného zájmu. Pojem „zájem“ je nutné odlišit od pojmu „účel zpracování“, které mohou být v praxi velmi podobné. Účel je konkrétní důvod pro zpracování osobních údajů, kdežto zájmem se rozumí širší zájem (užitek) správce při zpracování osobních údajů, nebo výhoda, kterou

181 ŽŮREK J. *Praktický průvodce GDPR*, op. cit. s. 83.
182 Recitál 47 GDPR.
183 Čl. 6 odst. 1 písm. f) a recitál 47 GDPR.
184 ŽŮREK J. *Praktický průvodce GDPR*, op. cit. s. 84.

může správci (nebo dokonce společnosti) přinést zpracování osobních údajů. Zájem musí být skutečný, měl by odpovídat aktuálně prováděné činnosti a nesmí být příliš neurčitý či spekulativní. V dalším kroku by mělo být vyhodnoceno, zda je daný zájem oprávněný, tedy jestli je v souladu s právem EU a vnitrostátním právním řádem.[185]

Poté musí správce provést posouzení, zda je zpracování osobních údajů skutečně nezbytné pro naplnění účelu určitého oprávněného zájmu. Pokud je zpracování vyhodnoceno jako nutné, pak dojde k samotnému poměřování oprávněných zájmů správce a základních práv a svobod subjektů údajů.[186]

Závislost použití oprávněného zájmu jakožto právního důvodu pro konkrétní zpracování osobních údajů na testu proporcionality či balančním testu zdůrazňuje i SDEU ve svých rozhodnutích, jako příklad lze uvést rozsudek SDEU z 24. listopadu 2011, ve věci C-468/10, Asociación Nacional de Establecimientos Financieros de Crédito v. Administración del Estado či relativně nový rozsudek SDEU ze 4. května 2017, ve věci C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas Satiksme“, ve kterém byla řešena sporná otázka, zda je policie povinna sdělit Rīgas Satiksme (dopravní podnik města Rigy) osobní údaje nezletilé osoby, vůči které chce uplatnit soukromoprávní nárok v občanskoprávním soudním řízení. SDEU ve zkratce dospěl k závěru, že příslušné ustanovení Směrnice 95/46/ES (čl. 7 písm. f) nestanoví policii povinnost takto osobní údaje zpřístupnit, ale jen oprávnění tak učinit, přičemž v daném případě by bylo legitimní údaje zpřístupnit za účelem ochrany oprávněných zájmů dopravního podniku. Uvedený článek Směrnice 95/46/ES však, dle SDEU, nebrání tomu, aby byly požadované údaje předány na základě vnitrostátního práva.[187]

V GDPR je uvedeno několik konkrétních příkladů oprávněných zájmů. Oprávněným zájmem je dle recitálu 47 GDPR např. zamezení podvodům, přímý marketing, dle recitálu 48 je oprávněným zájmem také předávání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely i zpracování osobních údajů zákazníků nebo zaměstnanců, v recitálu 49 je jako příklad oprávněného zájmu uvedeno zabránění neoprávněnému přístupu k sítím elektronických komunikací či zamezení škodám na počítačových systémech a systémech elektronických komunikací.

185 WP 29: Stanovisko č. 06/2014 *ke konceptu oprávněného zájmu dle čl. 7 Směrnice 95/46/ES* přijaté dne 9. dubna 2014.

186 Tamtéž.

187 NONNEMANN, F. *Aktuální judikatura SDEU k oprávněnému zájmu jako právnímu titulu pro zpracování osobních údajů*. Právní rozhledy 15-16/2017, s. 541.

I tento právní důvod má své místo při zpracování osobních údajů zaměstnavatelem jako správcem osobních údajů. Běžným případem, kdy se takový právní důvod pro zpracování osobních údajů ze strany zaměstnavatele uplatní, je často diskutované téma kontroly a sledování zaměstnanců. Sledováním zaměstnanců se přitom rozumí déle trvající nebo opakované systematické kontrolování zaměstnanců za pomoci určitého systému či prostředku, nikoliv jen kontrola zaměstnanců prováděná ad hoc.[188]

Sledování zaměstnanců je typickým případem, kdy sice existuje legitimní zájem zaměstnavatele do určité míry kontrolovat zaměstnance při výkonu práce (zavést sledovací opatření), chránit svůj majetek, ale proti těmto zájmům zaměstnavatele stojí základní práva zaměstnanců, zejména právo na soukromí, jež zahrnuje i právo zaměstnance na soukromí na pracovišti[189]. Přípustnost zavedení sledovacího opatření na pracovišti, za splnění určitých podmínek, dovodil i ESLP, a to např. ve známém rozsudku Bărbulescu proti Rumunsku (č. 61496/08) ze dne 12. ledna 2016, který se věnuje otázce využívání internetu pro soukromé účely během pracovní doby, resp. otázce monitoringu elektronické komunikace zaměstnance vedené během pracovní doby, to vše v souvislosti s výpovědí danou zaměstnavatelem z tohoto důvodu.

V každém případě platí, že vzhledem ke střetu práv zaměstnavatele a zaměstnance při zavedení sledovacích opatření, je vždy nutné poměřit, které z práv stojících proti sobě v daném případě převáží.

Za legitimní důvody k zavedení sledovacího opatření zaměstnavatelem lze považovat zejména ochranu života a zdraví zaměstnavatele, zaměstnance či jiných osob nacházejících se v kontrolovaném prostoru, ochranu majetku zaměstnavatele nebo jiných osob a kontrolu pracovní výkonnosti zaměstnance.[190]

Sledování zaměstnanců může být prováděno několika různými formami. Níže jsou blíže popsány jen dvě možné formy monitoringu zaměstnanců, a to monitorování e-mailové pošty a kamerové systémy na pracovišti. V zásadě lze ale říci, že obecná

188 MORÁVEK, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*, Právní rozhledy 17/2017, s. 573.

189 Srov. Rozhodnutí Evropského soudu pro lidská práva ve věci stížnosti č. 13710/88 *Niemietz v. Německo* ze dne 16. prosince 1992, ve kterém je mj. uvedeno následující *„Soud neshledává nezbytným ani nutným pokoušet se o vyčerpávající definici pojmu ‚soukromý život'. Bylo by však příliš restriktivním omezovat tento pojem na ‚vnitřní kruh', v jehož rámci může jednotlivec žít svůj vlastní osobní život podle libosti, a zcela z něho vyloučit vnější svět nezahrnutý do tohoto kruhu. Respektování soukromého života musí do určité míry zahrnovat právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi. Dále se pak zdá, že neexistuje důvod pro to, aby tento způsob chápání pojmu ‚soukromý život' vylučoval aktivitu profesní nebo obchodní povahy, protože právě během své pracovní činnosti má většina lidí značnou, ne-li největší příležitost rozvíjet vztahy s vnějším světem."*

190 NONNEMANN, F. *Soukromí na pracovišti*, Právní rozhledy 7/2015, s. 229.

pravidla a principy pro posuzování oprávněnosti dalších forem monitoringu, jako je monitoring telefonů, aktivity na PC, pomocí GPS, apod. budou obdobná.

Jednou z relativně problematických forem je monitorování e-mailové pošty zaměstnanců, které naráží zejména na zákaz porušení listovního tajemství zakotvený v čl. 13 LZPS. K pracovním e-mailovým adresám a k e-mailové korespondenci z hlediska možného monitoringu ze strany zaměstnavatele se vyjádřil i ÚOOÚ ve svém stanovisku č. 2/2009. ÚOOÚ zde mimo jiné uvádí, že pokud je e-mailová adresa patřící zaměstnavateli tvořená jménem a příjmením zaměstnavatele, budou e-maily na ní doručené soukromou elektronickou poštou a e-mailová adresa sama o sobě bude osobním údajem, jež oprávněně zpracovává zaměstnavatel. Naopak e-mailová adresa tvořená neutrálními označeními ve stylu help@obchodnífirma.cz je považována za úřední e-mailovou adresu, a to i v případě, že ji bude spravovat jen jeden zaměstnanec.[191] Podoba e-mailové adresy je však jen jedním z několika faktorů, které hrají roli při posuzování oprávněnosti sledování korespondence vedle oslovení, příjemce apod.[192]

ÚOOÚ ve výše uvedeném stanovisku dále stanovil, že zaměstnavatel není oprávněn sledovat, monitorovat a zpracovávat obsah korespondence zaměstnanců. Naopak je přípustné, aby zaměstnavatel sledoval počet doručených a odeslaných e-mailů, případně i včetně hlavičky e-mailů.[193] Takový postup zaměstnavatele lze legitimně odůvodnit právem sledovat u svých zaměstnanců dodržování pracovní doby a její využití.[194]

Zákaz zpracovávání obsahu korespondence zaměstnanců však neplatí bezvýhradně. Důležitá je v každém případě povaha e-mailu, pokud se bude jednat zřejmě o pracovní e-mail, měl by mít zaměstnavatel právo za určitých okolností otevřít a přečíst takový e-mail (i když bude doručen na e-mailovou adresu tvořenou jménem a příjmením zaměstnance) z důvodu ochrany svých práv.[195] Pokud např. zaměstnanec nebude přítomen na pracovišti a z důvodu jeho nepřítomnosti bude hrozit prodlení, které by mohlo mít dopad na majetkovou sféru zaměstnavatele, bude zaměstnavatel oprávněn

191 ÚOOÚ: Stanovisko č. 2/2009 *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*.

192 MORÁVEK, J. in PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 954. ISBN 978-80-7552-609-0.

193 ÚOOÚ: Stanovisko č. 2/2009 *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*.

194 BARTÍK V., JANEČKOVÁ, E. *Ochrana osobních údajů z pohledu zvláštních právních úprav k 1. 8. 2012*. 1. vydání. Olomouc: ANAG, 2012, s. 263, ISBN 978-80-7263-749-2.

195 ÚOOÚ: Stanovisko č. 2/2009 *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*.

otevřít a přečíst pracovní e-maily, aby předešel újmě na svém majetku. Bude se jednat o zákonné zpracování z důvodu ochrany oprávněných zájmů. Na druhou stranu platí, že pokud bude podle několika identifikačních znaků (odesílatel, oslovení, příjemce) patrné, že se jedná o čistě soukromou korespondenci zaměstnance, zaměstnavatel tuto nesmí otevřít ani číst.[196]

Další běžnou formou monitoringu zaměstnanců je zavedení kamerových systémů na pracovišti. Zaměstnavatelé kamerové systémy na pracoviště obvykle instalují za účelem sledování, jestli zaměstnanci plní své pracovní povinnosti a zda řádně využívají pracovní dobu a/nebo za účelem ochrany svého či svěřeného majetku (zejména za účelem předcházení krádežím či poškození majetku).[197] V úvahu připadá též instalace kamerového systému za účelem ochrany života a zdraví zaměstnanců či jiných osob, které se pohybují v prostoru snímaném kamerami.

Z hlediska ochrany osobních údajů zaměstnanců či jiných osob snímaných kamerami je, dle ÚOOÚ nutné rozlišit, zda se jedná o kamerové systémy provádějící záznam pořízených záběrů, nebo nikoliv. Pouze provozování kamerových systémů se záznamy je totiž považováno za zpracování osobních údajů ve smyslu ZOOÚ. Zároveň samozřejmě musí být splněna obecná podmínka, že zaznamenané údaje umožní přímou či nepřímou identifikaci určité fyzické osoby.[198]

V případě, že zaměstnavatel na pracovišti využije kamerový systém se záznamovým zařízením, bude se muset zpravidla řídit jak pravidly pro sledování zaměstnanců dle § 316 zákoníku práce, tak předpisy na ochranu osobních údajů. Při využití kamerových systémů, které neprovádí záznam pořízených záběrů, by se na zaměstnavatele měla vztahovat pouze úprava obsažená v zákoníku práce, neboť nebude provádět zpracování osobních údajů.[199] Za zmínku na tomto místě stojí, že dle dohody ÚOOÚ a Státního úřadu inspekce práce dohled nad dodržováním § 316 odst. 1 – 3 zákoníku práce vykonává inspekce práce, která má od 29. 7. 2017 také pravomoc zaměstnavatele za porušení tohoto ustanovení zákoníku práce sankcionovat.[200] Význam rozdílného právního režimu pro kamerové systémy se záznamem pořízených záběrů a bez tohoto záznamu se tak může v praxi stírat.

196 MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích. 1. vydání*, op. cit. s. 406.

197 BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi (vybrané problémy). 4. vydání*. Praha: Wolters Kluwer ČR, 2016, s. 124, ISBN 978-80-7552-141-5.

198 ÚOOÚ: Stanovisko č. 1/2006 *Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*.

199 NONNEMANN, F. *Soukromí na pracovišti*, Právní rozhledy 7/2015, s. 229.

200 MORÁVEK, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*, Právní rozhledy 17/2017, s. 573.

Kamerové systémy jakožto prostředek sledování zaměstnanců je do určité míry specifický tím, že představuje extrémně závažný zásah do soukromí. K této problematice se vyjádřil i Nejvyšší správní soud v rozhodnutí sp. zn. 5 As 158/2012 ze dne 23. srpna 2013, když uvedl mj. následující: *„k instalaci kamerových systémů, s ohledem na jejich povahu a zásah do osobní integrity osob, je možné přistoupit až tehdy, pokud už veškeré méně invazivní prostředky selhaly anebo by nebyly schopny naplnit vytyčený účel, který je sledován“.*

Ze znění § 316 odst. 2 zákoníku práce je možné dovodit, že na pracovišti by měl být kamerový systém zaveden jen tehdy, jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, což je pojem, který může v praxi působit problémy, neboť je poměrně obtížné vymezit, co lze označit jako „důvod spočívající ve zvláštní povaze činnosti zaměstnavatele“. Ani judikatura doposud nedovodila určitá obecná pravidla, která by mohla být aplikována při posouzení, zda může důvod zavedení sledovacích opatření naplňovat „důvod spočívající ve zvláštní povaze činnosti zaměstnavatele“. Lze se tak s názory, že zájem zaměstnavatele na ochraně svého majetku nelze sám o sobě považovat za závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, takovým důvodem by mohlo být např. pracoviště, kde se pracuje s citlivými informacemi, utajovanými skutečnostmi nebo vyššími majetkovými hodnotami.[201]

Na druhou stranu je ale třeba zdůraznit, že jsou běžné i situace, kdy zaměstnavatel zavede určité sledovací opatření (např. kamerový systém) nikoliv s cílem kontrolovat/sledovat zaměstnance, a tím zasahovat do jejich soukromí, ale za účelem ochrany majetku v obecné rovině (např. ochrana svěřeného vozidla) – ochrany oprávněného zájmu. V případech, kdy není sledovací opatření zřízeno vůbec za účelem sledování zaměstnance z hlediska nakládání se svěřenými pracovními nebo výrobními prostředky, ani za účelem kontroly dodržování pracovněprávních povinností ze strany zaměstnanců, by se měla aplikovat toliko úprava obsažená v právních předpisech na ochranu osobních údajů, případně též obecná právní úprava pracovněprávních vztahů, ale ne § 316 odst. 1 – 3 zákoníku práce.[202] Autorka se s tímto závěrem plně ztotožňuje a má za to, že v případě, kdy zaměstnavatel zavedením kontrolních/sledovacích prostředků nemá v úmyslu primárně kontrolovat zaměstnance z hledisek vyčtených

201 ZEMANOVÁ ŠIMONOVÁ, H. *Právní prostředky ochrany osobnosti zaměstnance.* Bulletin advokacie. 10/2016, s. 40.

202 MORÁVEK, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*, Právní rozhledy 17/2017, s. 573.

v předchozí větě, není nutné, aby se na něj vztahoval § 316 odst. 1 – 3 zákoníku práce, který kladně na zaměstnavatele jako správce osobních údajů do určité míry přísnější požadavky co do odůvodnění zavedení sledovacích mechanismů - naplnění podmínky závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele.

Oprávněnost zavedení kamerového systému na pracovišti ale bude třeba v každém případě posuzovat u každého jednotlivého případu zvlášť s využitím testu proporcionality.

3.3 Korektnost a transparentnost

Dalšími ze základních zásad, kterými je třeba se řídit při provádění zpracování osobních údajů, jsou zásady korektnosti a transparentnosti zakotvené spolu se zásadou zákonnosti v čl. 5 odst. 1 písm. a) GDPR.

Opět se jedná o zásady, které musely být při zpracování osobních údajů respektovány již před účinností GDPR. Ve Směrnici 95/46/ES byla mezi zásadami pro kvalitu údajů výslovně zakotvena pouze povinnost zpracovávat osobní údaje korektně a zákonným způsobem.[203] V ZOOÚ byly zásady korektnosti a transparentnosti v zásadě promítnuty do § 5 odst. 1 písm. g), který stanovil povinnost zpracovávat osobní údaje pouze otevřeně. Zásada transparentnosti tedy nebyla v ZOOÚ ani ve Směrnici 95/46/ES explicitně uvedena, nicméně, nad rámec výše uvedeného, oba tyto předpisy stanovily povinnost informovat subjekt údajů o zpracování jeho osobních údajů[204], z čehož lze též dovodit, že tato zásada ovládala zpracování osobních údajů i před účinností GDPR. Obsah zásady transparentnosti a zásady korektnosti je navíc takřka totožný, výslovné zakotvení povinnosti zpracovávat osobní údaje ve vztahu k subjektům údajů transparentně v GDPR tedy nelze považovat za nijak převratné.[205]

K samotnému vymezení zásad korektnosti a transparentnosti je nejdříve na místě uvést následující. Tyto zásady vyjadřují povinnost poskytovat subjektům údajů zejména informace o tom, kdo, v jakém rozsahu, jakým způsobem a za jakými čely zpracovává jejich osobní údaje, včetně informací o tom, komu jsou osobní údaje předávány. Subjekty údajů by dále měly být upozorněny na existující rizika, pravidla, záruky a práva v souvislosti se zpracováním jejich osobních údajů.[206] Základní myšlenka, která

203 Čl. 6 odst. 1. písm. a) Směrnice 95/46/ES.
204 Srov. čl. 10 - 12 Směrnice 95/46/ES a §§ 11 a 12 ZOOÚ.
205 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* op. cit. s. 107.
206 Recitál 39 GDPR.

stojí za zásadou transparentnosti i korektnosti je taková, že subjekt údajů by měl mít k dispozici veškeré informace tak, aby mohl s předstihem poznat rozsah a důsledky zpracování jeho osobních údajů a aby nebyl později překvapen způsobem a rozsahem nakládání s jeho osobními údaji.[207]

Zásada transparentnosti je promítnuta a rozvedena zejména v ustanoveních, která ukládají správci konkrétní povinnosti informovat subjekt údajů o prováděném zpracování. Informační povinnost vůči subjektům údajů je jednou ze základních, a v praxi možná i nejdůležitějších, povinností správce osobních údajů, a je blíže specifikována zejména v čl. 12 – 14 GDPR. Zásada transparentnosti se projeví, i v případě dalších sdělení činěných správcem vůči subjektům údajů, jak bude přiblíženo níže.

V čl. 12 odst. 1 GDPR je blíže rozveden způsob, jakým mají být informace, které je správce povinen subjektům údajů sdělit, těmto subjektům předány. Sdělení by mělo být především provedeno stručným, transparentním, srozumitelným a snadno přístupným způsobem.

Správci by měli subjektům údajů poskytovat informace efektivně tak, aby nedošlo k zahlcení informacemi, zároveň by informace týkající se zpracování osobních údajů měly být odděleny od jiných údajů (např. od jiných smluvních ustanovení). Požadavek srozumitelnosti sdělení bude naplněn, pokud sdělení učiněnému správcem porozumí průměrná osoba v rámci cílové skupiny, vychází se přitom z toho, že správce ví, jaká je jeho cílová skupina, tedy čí osobní údaje zpracovává a je schopen vyhodnotit, jakým způsobem musí informace podat, aby byly pro subjekty údajů srozumitelné. Se srozumitelností je pak svázán i požadavek na použití jasných a jednoduchých jazykových prostředků (např. nevyužívání složitých souvětí, vyhýbání se podmiňovacímu způsobu). Informace by měly být pro subjekty údajů také snadno přístupné, tedy subjektu údajů by mělo být jednoduše zřejmé, jak se dostane k informacím o nakládání s jeho osobními údaji (např. uvedením odkazu, poskytnutím požadovaných informací napřímo).[208]

Co se týče formy sdělení subjektům údajů, dle čl. 12 odst. 1 GDPR, je základní forma písemná, GDPR, ale nevylučuje ani využití jiných, blíže nespecifikovaných prostředků, včetně elektronické formy, nebo ústní formy (požádá-li o to subjekt údajů a je-li jeho identita prokázány jiným způsobem, nikoliv jenom prohlášením dané osoby).

207 WP29: *Pokyny k transparentnosti podle nařízení 2016/679* přijaty dne 29. listopadu 2017, ve znění naposledy revidovaném a přijatém dne 11. dubna 2018.
208 WP29: *Pokyny k transparentnosti podle nařízení 2016/679*, op. cit.

V souladu s čl. 12 odst. 5 GDPR musí být veškerá sdělení správce dle čl. 13 a 14 GDPR a také veškeré úkony dle čl. 15 – 22 a čl. 34 poskytována/činěny bezplatně s výjimkou toho, kdy se jedná o nedůvodné nebo nepřiměřené žádosti subjektu údajů (např. jsou-li opakované).

Běžně bývá informační povinnost vůči subjektům údajů plněna prostřednictvím dokumentu označeného jako „Privacy Policy“ (česky bývá takový dokument pojmenováván „Zásady ochrany soukromí“ či „Zásady zpracování osobních údajů“ apod.) obsahujícího veškeré informace, které by správci měli subjektům údajů sdělovat v souvislosti se zpracováváním jejich osobních údajů; takový dokument je v ideálním případě dostupný v elektronické formě na webových stránkách příslušného správce a subjekt údajů se tak s ním může kdykoliv seznámit (i před tím, než dojde ke zpracování jeho osobních údajů) a dle potřeby se k němu kdykoliv v budoucnosti vracet. WP29 se přiklání k závěru, že pokud správce zpřístupní informace a sdělení adresované subjektům údajů prostřednictvím svých webových stránek, je vhodné použít formu vícevrstevných prohlášení/oznámení o ochraně soukromí, která návštěvníkům webových stránek umožňují přejít na konkrétní části prohlášení/oznámení, která subjekt aktuálně hledá.[209]

Autorka považuje tento způsob plnění informační povinnosti správce vůči subjektům údajů za nejvhodnější řešení, a to zejména pro správce, kteří zpracovávají osobní údaje velkého počtu subjektů (typicky pokud se jedná o informování subjektů údajů, jimž správce např. poskytuje služby/prodává zboží a v souvislosti s tím zpracovává jejich osobní údaje), samozřejmě za předpokladu, že správce provozuje webové stránky. Nelze jej ale efektivně využít ve všech případech, vždy bude záležet na povaze činnosti správce, účelu a důvodu zpracování a okruhu subjektů údajů.

V čl. 13 a 14 GDPR je obsažen výčet kategorií informací, které je správce osobních údajů povinen poskytnout v souvislosti se zpracováním osobních údajů subjektu těchto údajů. Čl. 13 dopadá na případy, kdy správce osobní údaje získá přímo od subjektu údajů (např. vědomé poskytnutí osobních údajů správci v souvislosti s uzavřením smlouvy, sledování subjektu údajů za pomoci kamery) a čl. 14 se správce musí řídit za situace, kdy osobní údaje získá jinak, než od subjektu údajů (např. z veřejně dostupných zdrojů, od zprostředkovatele údajů).

Správce je povinen v souvislosti se zpracováním osobních údajů jejich subjektům vždy poskytnout následující informace: totožnost a kontaktní údaje správce,

209 WP29: *Pokyny k transparentnosti podle nařízení 2016/679*, op. cit.

případně kontaktní údaje pověřence pro ochranu osobních údajů, účely a právní základ zpracování (popřípadě i oprávněné zájmy správce nebo třetí, jde-li o zpracování založené na čl. 6 odst. 1 písm. f) GDPR), údaje o příjemcích nebo kategorií příjemců osobních údajů, úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci. Správce je povinen poskytnout subjektu údajů i další informace za předpokladu, že jsou nutné pro zajištění spravedlivého a transparentního zpracování, jedná se mj. o dobu, po kterou budou osobní údaje uloženy, případně kritéria pro její stanovení, údaj o existenci práva subjektu požadovat od správce přístup k jeho osobním údajům, jejich opravu, výmaz, případně omezení zpracování, vznést námitku proti zpracování, údaj o existenci práva na přenositelnost údajů či práva podat stížnost u dozorového úřadu.

Seznamy informací obsažených v čl. 13 a 14 GDPR, jejichž neúplný výčet je uveden v předchozím odstavci, jsou do velké míry totožné (výjimkou je např. povinnost sdělit kategorie dotčených osobních údajů, která je relevantní jen pro případ, kdy správce nezíská osobní údaje od subjektu, a subjekt údajů logicky nemusí vědět, jaké osobní údaje správce získal).

Dle WP29 by v případech, kdy bude docházet ke složitému, technicky náročnému nebo neočekávanému zpracování osobních údajů, měli správce kromě informací vyčtených v čl. 13 a 14 GDPR zdůraznit odděleně nejdůležitější důsledky zamýšleného zpracování.[210]

Existují i okolnosti, za kterých správce osobních údajů nebude povinen informovat subjekty o zpracování jejich osobních údajů dle čl. 13 a 14 GDPR. V čl. 13 odst. 4 GDPR je stanoveno, že správce se předchozími odstavci daného článku nemusí řídit, pokud subjekt údajů dané informace již má k dispozici, avšak výjimka z informační povinnosti se uplatní jen do míry odpovídající rozsahu informací, které subjekt údajů má.

V čl. 14 GDPR je okruh výjimek, kdy správce nemusí poskytnout subjektu informace o zpracování jeho osobních údajů, širší. Kromě výše popsané skutečnosti, tedy že subjekt požadované informace již má, jsou v čl. 14 odst. 5 GDPR uvedeny další tři případy odůvodňující vynětí z informační povinnosti dle tohoto článku. Jeden z takových případů nastane, pokud se ukáže, že poskytnutí informací dle čl. 14 není možné, nebo by vyžadovalo nepřiměřené úsilí (to se dotýká např. zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely statistického výzkumu), anebo

210 WP29: *Pokyny k transparentnosti podle nařízení 2016/679*, op. cit.

je-li pravděpodobné, že by požadované poskytnutí informací znemožnilo nebo výrazně ztížilo dosažení cílů daného zpracování. Dalším důvodem je situace, kdy je získávání nebo zpřístupnění osobních údajů výslovně stanoveno právem EU nebo vnitrostátní právní úpravou vztahující se na správce za splnění podmínky, že v takovém právním předpise jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektů údajů. Poslední výjimkou je pak případ, kdy osobní údaje musí zůstat důvěrné vzhledem k povinnosti zachovávat služební tajemství dle práva EU nebo členského státu, což zahrnuje i zákonnou povinnost mlčenlivosti.

Co se týče lhůty, ve které by měl správce splnit povinnost informovat subjekt o zpracování osobních údajů v rozsahu dle čl. 13 a 14 GDPR, platí, že v případě, kdy jsou osobní údaje získány přímo od subjektu údajům, měl by správce požadované informace poskytnout v okamžiku získání osobních údajů.[211]

Za situace, kdy správce nezíská osobní údaje od subjektu, měl by předepsané informace subjektu údajů obecně předat v přiměřené lhůtě od získání osobních údajů, nejpozději však do jednoho měsíce. Obecná jednoměsíční lhůta může být zkrácena, pokud mají být osobní údaje použity pro účely komunikace se subjektem údajů, kdy platí, že správce musí informační povinnost splnit nejpozději v momentu první komunikace s tímto subjektem. Tato lhůta může být rovněž zkrácena, pokud mají být osobní údaje subjektu zpřístupněny jinému příjemci, kdy je správce povinen poskytnout subjektu informace dle čl. 14 GDPR nejpozději při prvním zpřístupnění osobních údajů.[212] Dle názoru WP29 by nicméně správci měli, pokud to bude možné, poskytnout subjektům údajů požadované informace s velkým předstihem před uplynutím výše uvedených lhůt, a to za účelem naplnění zásady korektnosti.[213]

Pokud v průběhu provádění zpracování osobních údajů dojde ke změnám v údajích, které je správce povinen dle čl. 13, resp. 14 GDPR sdělovat subjektům údajů, měl by správce, v souladu se zásadou transparentnosti a korektnosti, dostatečně důrazně a včas upozornit subjekty údajů na tyto změny, včetně jejich dopadu na subjekty údajů.[214]

Kromě splnění informační povinnosti dle čl. 13 a 14 GDPR, musí správci osobních údajů zásadu transparentnosti dodržovat také při komunikaci se subjekty údajů v souvislosti s jejich právy dle čl. 15 – 22 GDPR (právo na přístup k osobním údajům,

211 Čl. 13 odst. 1 GDPR.
212 Čl. 14 odst. 3. písm. a) – c) GDPR.
213 WP29: *Pokyny k transparentnosti podle nařízení 2016/679*, op. cit.
214 WP29: *Pokyny k transparentnosti podle nařízení 2016/679*, op. cit.

právo na opravu, výmaz – „právo být zapomenut“, právo na omezení zpracování, na přenositelnost údajů, právo vznést námitku, právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování) a čl. 34 GDPR (oznamování případů porušení zabezpečení osobních údajů subjektu údajů) GDPR a měli by dbát na usnadňování výkonu práv subjektů dle čl. 15 – 22 GDPR. Při činění sdělení dle čl. 15 – 22 a 34 GDPR musí správce dodržovat stejná pravidla jako při plnění informační povinnosti dle čl. 13 a 14 GDPR, jak je popsáno výše.

Autorka závěrem shrnuje, že zásada korektnosti a transparentnosti jsou jedny z nejvýznamnějších zásad, které ovládají zpracování osobních údajů a zahrnují několik povinností, které vyžadují od správce v praxi konkrétní aktivní jednání vůči subjektům údajů za účelem jejich naplnění.

Autorka také konstatuje, že s účinností GDPR došlo k rozšíření, lépe řečeno ke zpřesnění katalogu povinností správce, které jsou projevem zásad korektnosti a transparentnosti. GDPR obsahuje detailnější přehled informací, které je správce povinen subjektům údajů sdělit v okamžiku získání osobních údajů dle čl. 13 GDPR, resp. v přiměřené lhůtě pro získání osobních údajů podle čl. 14 GDPR.

Přehledněji a detailněji jsou v GDPR vymezena též jednotlivá práva subjektů údajů související se zpracováním jejich osobních údajů, úplně nově je v GDPR obsaženo např. právo subjektu na přenositelnost údajů (čl. 20 GDPR). Další novinkou související s výkonem práv subjektů údajů je výslovné uvedení práva správce odmítnout nebo zpoplatnit zjevně nedůvodné nebo nepřiměřené žádosti subjektu údajů v souladu s čl. 12 odst. 5 GDPR. Objevují se názory, že GDPR přineslo obecné posílení systému práv subjektů údajů.[215] Proti tomuto názoru lze však namítat, že většina práv již byla obsažena v předchozí právní úpravě, a to buď výslovně (např. právo na opravu osobních údajů, právo na přístup ke kopii zpracovávaných osobních údajů) nebo byla dovozena judikaturou (právo na výmaz, které bylo formulováno v rozhodnutí SDEU ve věci C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González).[216]

215 Srov. *ÚOOÚ: Základní příručka k GDPR, 6. Práva subjektu údajů*, dostupné na https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744.

216 MATYSOVÁ, M., NONNEMANN, F., *Možnost odmítnout uplatnění práva subjektu údajů dle GDPR.* Právní rozhledy 12/2018, s. 424.

3.4 Účelové omezení

Zásada účelového omezení je vyjádřena v čl. 5 odst. 1. písm. b) GDPR, který stanoví, že *osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely*. Tato zásada byla zakotvena již ve Směrnici 95/46/ES, a to v čl. 6 odst. 1. písm. b), jehož znění bylo přejato do GDPR jen s drobnými změnami. V ZOOÚ je zásada účelového omezení zmíněna v § 5 odst. 1 písm. a), f) a h).

Vymezení účelu, pro který mají být osobní údaje zpracovány, je jednou ze základních povinností správce. Správce tím vyjadřuje důvod, proč má v úmyslu osobní údaje zpracovávat, a zpravidla je oprávněn provádět zpracování osobních údajů výhradně za účelem, který si stanovil. Od vymezení účelu zpracování osobních údajů se odvíjejí také další zásady zpracování jako je minimalizace údajů a omezení uložení.[217]

Správce by měl vymezit účel zpracování nejpozději v okamžiku shromažďování osobních údajů.[218] Při stanovení účelu musí správce dbát na to, aby byl tento dostatečně určitý, výslovně vyjádřený a legitimní. Určitost účelu znamená takovou specifikaci, která umožní rozlišit, jaké zpracování bude či nebo na základě tohoto účelu probíhat a zároveň bude možné jednoduše posoudit soulad účelu s právními předpisy. Účel by neměl být vymezen příliš vágně, dle názoru WP29 kritérium určitosti nebude obvykle splněno, pokud bude účel vymezen obecnými termíny typu „marketingové účely“, „bezpečnost IT“ apod.[219]

Jak již bylo nastíněno výše, účel zpracování musí být také výslovně vyjádřen, tedy musí být vyjádřen v určité srozumitelné formě, a to tak, aby jej pochopili stejně zpracovatelé, které správce využívá, subjekty údajů, ale i dozorové úřady. Na vyjádření účelu zpracování se vztahují pravidla, která jsou zahrnuta v zásadě transparentnosti popsané výše v této práci. Konečně platí, že účel zpracování musí být vždy legitimní. Legitimita účelu neznamená jen požadavek, aby bylo zpracování založeno vždy na některém z právních základů pro zpracování uvedených v čl. 6 GDPR, ale zahrnuje i

217 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* op. cit. s. 107.
218 Recitál 39 GDPR.
219 WP29: Stanovisko č. 3/2013 *k účelovému omezení* přijaté dne 2. dubna 2013.

podmínku, aby byl účel v souladu s právními předpisy na ochranu osobních údajů i s jinými obecně závaznými právními předpisy vztahujícími se na daného správce.[220]

Jakmile je stanovený účel zpracování naplněn a neexistuje-li jiný právní titul pro zpracování osobních údajů, správce by měl prováděné zpracování ukončit a zpracovávané osobní údaje zlikvidovat.

Výjimku z povinnosti zpracovávat osobní údaje jen za stanoveným účelem tvoří tzv. další zpracování (zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely), které může být prováděno i nad rámec původního účelu zpracování.[221]

Se zásadou účelového omezení je spojena i povinnost správce zavést vhodná technická a organizační opatření k zajištění toho, že bude standardně docházet jen ke zpracování takových osobních údajů, které jsou pro konkrétní účel předmětného zpracování nezbytné zakotvená v čl. 25 odst. 2 GDPR.

3.5 Minimalizace údajů

Jak bylo uvedeno výše, od zásady účelového omezení se odvíjí zásada minimalizace údajů. V souladu s touto zásadou musí být zpracovávány osobní údaje *přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány*.[222] Zásada minimalizace údajů byla obdobně formulována i v čl. 6 odst. 1. písm. c) Směrnice 95/46/ES a byla promítnuta též do § 5 odst. 1 písm. d) ZOOÚ.

Správce by měl při stanovení účelu zároveň vymezit i rozsah osobních údajů, které bude nutné zpracovávat za stanoveným účelem. Rozsah osobních údajů by měl být stanoven skutečně jako nezbytný ve vztahu k danému účelu, tedy tak, že zpracovávané osobní údaje budou stačit k dosažení konkrétního účelu, ale nebudou zahrnovat žádné nadbytečné údaje, které by správce pro daný účel nevyužil.[223] Tímto by měl být eliminován nepřiměřený zásah do soukromí subjektů údajů.

Některé zvláštní předpisy zásadu minimalizace údajů zdůrazňují, jako např. zákoník práce, konkrétně pak jeho § 30 odst. 2 obsahující obecný zákaz, aby zaměstnavatel požadoval od osoby ucházející se o zaměstnání údaje bezprostředně nesouvisející s uzavřením pracovní smlouvy a § 316 odst. 4, ve kterém je uveden

220 WP29: Stanovisko č. 3/2013 *k účelovému omezení*, op. cit.
221 ŽŮREK J. *Praktický průvodce GDPR*. 2017, op. cit. s. 62.
222 Čl. 5 odst. 1. písm. c) GDPR.
223 POSPÍŠIL, D. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. op. cit. s. 115 - 116.

demonstrativní výčet údajů, které zaměstnavatel zpravidla nesmí od zaměstnance požadovat za trvání pracovněprávního vztahu, a to z toho důvodu, že bezprostředně nesouvisí s výkonem práce a s pracovním poměrem (jedná se např. o informace o těhotenství, majetkových poměrech, členství v odborové organizaci či trestněprávní bezúhonnosti). Zákaz požadovat určité informace po zaměstnancích dle § 316 odst. 4 zákoníku práce by se přitom měl logicky vztahovat i na uchazeče o zaměstnání, neboť nesmí-li zaměstnavatel požadovat takové údaje po svých zaměstnancích, tím spíše by je neměl vyžadovat od uchazečů o zaměstnání. Demonstrativní výčet zakázaných informací obsažený v § 316 odst. 4 zákoníku práce se navíc částečně překrývá s přehledem informací, které nesmí zaměstnavatel požadovat při výběru zaměstnanců, obsaženým v § 12 odst. 2 zákona č. 435/2004 Sb., o zaměstnanosti (např. pokud jde o údaj o sexuální orientaci či členství v odborových organizacích).[224]

3.6 Přesnost

Čl. 5 odst. 1. písm. d) GDPR zakotvuje povinnost správce zpracovávat pouze přesné a dle potřeby aktualizované osobní údaje a dále povinnost přijmout veškerá rozumná opatření, aby nepřesné osobní údaje byly bezodkladně vymazány nebo opraveny. Opět se nejedná o žádnou novinku mezi zásadami zpracování osobních údajů, když zásada přesnosti byla zakotvena již v čl. 6 odst. 1 písm. d) Směrnice 95/46/ES a § 5 odst. 1 písm. c) ZOOÚ.

Zásada přesnosti předpokládá, že pokud v průběhu zpracování osobních údajů správce narazí na osobní údaje, které budou zjevně nepřesné, nebo obdrží-li žádost subjektu údajů, musí přijmout potřebná opatření, aby, s přihlédnutím k účelům zpracování, byly nepřesné osobní údaje buď vymazány, nebo opraveny.[225]

Jako nepřesné je možné označit údaje, které jsou gramaticky nesprávné, ale také formálně správné údaje zpracované v souvislosti s nesprávnou informací (např. zpracování správných identifikačních údajů osoby spolu společně s informací, že tato osoba je dlužníkem, i když ve skutečnosti dlužníkem není).

GDPR, stejně jako dříve Směrnice 95/46/ES a ZOOÚ požadují, aby správce prováděl aktualizaci zpracovávaných osobních údajů, tedy nápravu zjištěných nesprávností, pakliže je to nezbytné vzhledem k účelu zpracování. Správce přitom

224 BĚLINA, M. in BĚLINA, M. a kol. *Pracovní právo,* 6. vydání, Praha: C. H. Beck, 2014, s. 170 – 171. ISBN 978-80-7400-283-0.
225 ŽŮREK J. *Praktický průvodce GDPR*. 2017, op. cit. s. 64.

nemusí kontrolu správnosti jím zpracovávaných osobních údajů provádět nepřetržitě, správce by měl sám vyhodnotit, jakým způsobem a v jakých intervalech bude kontrolu provádět.[226]

Zásada přesnosti se odráží zejména v čl. 16 GDPR upravujícím právo subjektu údajů na opravu nepřesných osobních údajů, které se ho týkají, ale i v čl. 18 odst. 1. písm. a) GDPR, který zakotvuje právo subjektu údajů požadovat po správci, aby omezil zpracování jeho osobních údajů, popírá-li subjekt údajů přesnost zpracovávaných osobních údajů, a to na dobu potřebnou pro správce k ověření přesnosti osobních údajů.

3.7 Omezení uložení

V souladu se zásadou omezení uložení vyjádřenou v čl. 5 odst. 1. písm. e) GDPR platí, že osobní údaje nesmí být v podobě umožňující identifikaci subjektů údajů uloženy déle, než je nezbytné pro naplnění účelu zpracování. Obdobně jako v případě zásady účelového omezení platí, že osobní údaje je možné uložit i po delší dobu, budou-li zpracovávány výlučně pro účely archivace ve veřejném zájmu, vědeckého nebo historického výzkumu či pro statistické účely podle čl. 89 odst. 1 GDPR. Tato zásada byla explicitně stanovena též ve Směrnici 95/46/ES, konkrétně v čl. 6 odst. 1. písm. e) a v ZOOÚ v § 5 odst. 1 písm. e).

Dobu uchování osobních údajů je zpravidla povinen určit sám správce, nejedná-li se o zpracování za účelem plnění zákonných povinností správce. V tomto případě zákon ukládající správci povinnost, k jejímuž splnění je nutné provádět zpracování osobních údajů, obvykle stanoví i přípustnou dobu zpracování. Příkladem je povinnost zaměstnavatele uchovávat mzdové listy zaměstnanců po dobu 30 kalendářních let následujících po roce, jehož se týkají, stanovená v § 35a odst. 4 písm. d) zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení.[227]

Při výkladu zásady omezení uložení je nutné reflektovat právo subjektu údajů na výmaz zakotvené v čl. 17 GDPR, které znamená povinnost správce provést výmaz osobních údajů týkající se subjektu za předpokladu, že existuje jeden z důvodů vyčtených v odst. 1 tohoto článku. Typickým důvodem bude právě uplynutí doby, po kterou bylo nutné osobní údaje zpracovávat k naplnění účelu zpracování. V některých

226 ÚOOÚ *K problematice aktualizace zpracovávaných osobních údajů*. Dostupné na https://www.uoou.cz/k-problematice-aktualizace-zpracovavanych-osobnich-udaju/d-1595.
227 NOVÁKOVÁ, L. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. op. cit. s. 118 - 119.

případech může dojít z důvodu existence práva subjektu údajů na výmaz k likvidaci údajů dříve než po uplynutí původně stanovené doby uložení osobních údajů.[228]

Likvidace nemusí být přitom provedena jen formou faktického výmazu osobních údajů, lze provést i jejich anonymizaci. Anonymizované údaje by pak již nenáležely do působnosti právních předpisů na ochranu osobních údajů, a správce by s nimi mohl dále pracovat, pokud by to pro něj bylo užitečné.

3.8 Integrita a důvěrnost

Poslední zásadou uvedenou ve výčtu v čl. 5 odst. 1. GDPR je zásada integrity a důvěrnosti. Tato zásada vyjadřuje povinnost zpracovávat osobní údaje takovým způsobem, aby bylo zajištěno jejich náležité zabezpečení, a to za použití vhodných technických nebo organizačních opatření chránících před neoprávněným zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

Povinnost zabezpečit osobní údaje zahrnuje povinnost zajistit ochranu před riziky ohrožujícími osobní údaje jak uvnitř organizace provádějící zpracování osobních údajů, tak vně této organizace a dotýká se zpracování prováděného ve všech podobách (jak automatizovaného, tak v papírové formě).[229]

Zásada integrity a důvěrnosti je rozvedena zejména v čl. 32 GDPR, který obsahuje konkrétní pravidla pro zabezpečení osobních údajů.

Oproti Směrnici 95/46/ES a ZOOÚ je zásada integrity a důvěrnosti zařazena k základním zásadám zpracování osobních údajů, což lze chápat jako zdůraznění toho, že povinnost zajistit náležité zabezpečení osobních údajů je nutné považovat za jednu ze základních povinností v souvislosti se zpracováním osobních údajů. Před účinností GDPR byla zásada integrity a důvěrnosti v podstatě vyjádřena v ustanoveních Směrnice 95/46/ES a ZOOÚ týkajících se přímo zabezpečení osobních údajů.[230] Povinnost zajistit bezpečnost zpracování osobních údajů byla nastíněna též v recitálu 46 Směrnice 95/46/ES.

228 DETLEV, G., HICKMAN T., *Chapter 6: Data Protecting Principles – Unlocking the EU General Data Protection Regulation*, 22. 7. 2016, dostupné na https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection.

229 JANEČKOVÁ E., *GDPR. Praktická příručka implementace*. Praha: Wolters Kluwer ČR, a.s., 2018, s. 9. ISBN 978-80-7552-248-1.

230 Srov. čl. 16 a 17 Směrnice 95/46/ES a § 13 ZOOÚ.

4 Vybrané povinnosti zaměstnavatele jako správce osobních údajů

V poslední kapitole této diplomové práce se autorka bude věnovat některým vybraným povinnostem, které musí zaměstnavatel jakožto správce osobních údajů dodržovat, s tím, že popsány budou vybrané povinnosti, které GDPR přináší buď zcela nově, nebo podstatně mění či rozšiřuje jejich koncept.

Jak již bylo uvedeno v první kapitole této práce, mezi povinnosti správců a zpracovatelů dle GDPR označované jako nové je možné zařadit povinnost vést záznamy o činnostech zpracování, jmenovat pověřence pro ochranu osobních údajů, provádět posouzení vlivu na ochranu osobních údajů a předchozí konzultace s dozorovým úřadem a též povinnost ohlašovat porušení zabezpečení osobních údajů dozorovému

úřadu a subjektu údajů. Z těchto povinností budou níže v této kapitole blíže rozebrány povinnosti vést záznamy o činnostech zpracování, provádět posouzení vlivu na ochranu osobních údajů a jmenovat pověřence pro ochranu osobních údajů, tedy povinnosti, které se nebudou nutně vztahovat na všechny správce či zpracovatele.

4.1 Záznamy o činnostech zpracování

První povinností správce (a též zpracovatele) zakotvenou v GDPR, která bude v této kapitole práce konkrétněji popsána, je povinnost vést záznamy o činnostech zpracování. Povinnost vést záznamy o činnostech zpracování, včetně stanovení minimálních požadavků na obsah takových záznamů a stanovení okruhu správců a zpracovatelů, na které se tato povinnost vztahuje, lze nalézt v čl. 30 GDPR. Záznamy o činnostech zpracování mají být komplexním dokumentem obsahujícím přehled o prováděném zpracování osobních údajů a jeho jednotlivých aspektech.

Jak bylo uvedeno výše, povinnost vést záznamy o činnostech zpracování Směrnice 95/46/ES ani ZOOÚ neznaly. Jedinou povinností vymezenou již v ZOOÚ, která má určitou souvislost s povinností vést záznamy o činnostech zpracování, je povinnost vést dokumentaci ohledně přijatých a provedených technicko-organizačních opatření k zajištění ochrany osobních údajů v souladu se ZOOÚ a jinými právními předpisy dle § 13 odst. 2 ZOOÚ. Jak již ale napovídá znění § 13 odst. 2 ZOOÚ, vedení dokumentace se týkalo jen zabezpečení osobních údajů prováděné skrze technicko-organizační opatření, což je dnes, dle GDPR, pouze jednou ze součástí obsahu záznamů o činnostech zpracování.[231]

Povinnost vést záznamy o činnostech zpracování bývá často označována jako částečné nahrazení oznamovací povinnosti dle § 16 ZOOÚ, která byla s účinností GDPR zrušena.[232] Záznamy o činnostech zpracování však, na rozdíl od oznámení dle § 16 ZOOÚ, správce nemusí předkládat dozorovému úřadu před zahájením zpracování osobních údajů, nicméně tyto samostatně vede a dozorovému úřadu je předloží až na jeho žádost. Dalším, poměrně podstatným rozdílem mezi vedením záznamů o činnostech zpracování dle čl. 30 GDPR a oznamovací povinností dle § 16 ZOOÚ, je

231 MALIŠ, P. *GDPR - 3. díl: Vedení záznamů o činnostech zpracování osobních údajů*. IT Systems č. 10/2017, dostupné na http://www.pravoit.cz/novinka/gdpr-3-dil-vedeni-zaznamu-o-cinnostech-zpracovani-osobnich-udaju.

232 Srov. JANEČKOVÁ, E., *GDPR. Praktická příručka implementace*. Op cit. s. 27 nebo NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: GRADA Publishing, a.s., 2018, s. 31. ISBN 978-80-271-0668-4 nebo ÚOOÚ: *Základní příručka k GDPR*, 2. *Nové přístupy a povinnosti*. Dostupné na https://www.uoou.cz/2-nove-p-istupy-a-povinnosti/d-27268.

skutečnost, že oznamovací povinnost se vztahovala toliko na správce osobních údajů, kdežto povinnost vést záznamy o činnostech zpracování se vztahuje jak na správce, tak na zpracovatele osobních údajů.[233]

Účel vedení záznamů o činnostech zpracování vyplývá z recitálu 82 GDPR, kdy platí, že za hlavní účel vedení záznamů o činnostech zpracování lze označit možnost správce (či zpracovatele) využít záznamy o činnostech zpracování k doložení souladu prováděného zpracování s GDPR. Jedná se tak o jeden z projevů zásady odpovědnosti správce dle čl. 5 odst. 2 GDPR, která zahrnuje povinnost správce být schopen doložit soulad zpracování se základními zásadami zpracování osobních údajů.[234]

Rozsah informací vedených v záznamech o činnostech zpracování se liší dle toho, zda záznamy vede správce nebo zpracovatel. V případě správce je minimální rozsah informací, které musí záznamy obsahovat, logicky širší. V souladu s čl. 30 odst. 1 písm. a) – g), musí záznamy vedené správce obsahovat minimálně tyto informace: jméno a kontaktní údaje správce (případně též společného správce, zástupce správce či pověřence pro ochranu osobních údajů), účely zpracování, kategorie subjektů údajů a osobních údajů, kategorie příjemců údajů, informace o předání údajů do třetí země nebo mezinárodní organizaci, plánované lhůty pro výmaz kategorií údajů, je-li to možné a popis technických a organizačních bezpečnostních opatření, je-li to možné. Zpracovatel musí do záznamů o činnostech zpracování zanést minimálně tyto informace: jméno a kontaktní údaje zpracovatele a správce, pro kterého zpracovatel jedná (případně také zástupce správce nebo zpracovatele či pověřence pro ochranu osobních údajů), kategorie zpracování, která zpracovatel provádí pro každého ze správců, informace o předání údajů do třetí země nebo mezinárodní organizaci a popis technických a organizačních bezpečnostních opatření, je-li to možné.

Forma záznamů o činnostech zpracování musí být písemná, čímž se ale rozumí i elektronická forma.

Poněkud problematický je čl. 30 odst. 5 GDPR, který stanoví okruh správců a zpracovatelů a jimi prováděného zpracování, na které se obecná povinnost vést záznamy o činnostech zpracování nevztahuje. Na prvním místě je mezi výjimkami z povinnosti vést záznamy o činnostech zpracování uvedeno, že tato povinnost se neaplikuje na podniky nebo organizace s méně než 250 zaměstnanci, což by samo o sobě naznačovalo, že povinnost vést záznamy o činnostech zpracování by se měla dotýkat jen

233 Recitál 82 GDPR.
234 MALIŠ, P. *GDPR - 3. díl: Vedení záznamů o činnostech zpracování osobních údajů*, op. cit.

velkých korporací. Text předmětného odstavce ale dále pokračuje tak, že výjimka pro správce či zpracovatele s méně než 250 zaměstnanci se nepoužije v případě, že prováděné zpracování pravděpodobně představuje riziko pro práva a svobody subjektů údajů, prováděné zpracování není příležitostné, nebo dochází-li ke zpracování zvláštních kategorií osobních údajů či údajů týkajících se rozsudků v trestních věcech a trestných činů.[235]

Výčet těchto dalších výjimek by pak striktním výkladem v podstatě činil výjimku z povinnosti vést záznamy o činnostech zpracování pro správce a zpracovatele s méně než 250 zaměstnanci v praxi nepoužitelnou. Aby mohlo být použito kritérium 250 zaměstnanců, muselo by totiž současně platit mj., že správce (zpracovatel) zpracovává osobní údaje jen příležitostně a dále nezpracovává žádné zvláštní kategorie osobních údajů, což v zásadě není reálné. Lze učinit závěr, že každý správce nebo zpracovatel, který jako zaměstnavatel zpracovává osobní údaje byť jen jednoho zaměstnance, provádí soustavné, nikoliv jen příležitostné zpracování osobních údajů, a to v souvislosti s vedením personální agendy (zpracování mezd, plnění povinností vůči orgánům státní správy apod.), o kterém by měl vést záznamy. Správce či zpracovatel jakožto zaměstnavatel také zpravidla zpracovává některý z údajů spadajících do zvláštní kategorie osobních údajů ve smyslu čl. 9 GDPR (typicky údaj o zdravotním stavu v případě nemocenské, pracovního úrazu, nemoci z povolání).[236]

Objevují se však i názory, že čl. 30 odst. 5 GDPR je nutné vykládat v souladu s jeho účelem, kterým nebylo stanovení výjimek tak, aby se v praxi mohly vztahovat jen na početně velmi omezenou skupinu správců a zpracovatelů.[237] Povinnost vést záznamy o činnostech zpracování by se, dle některých autorů, měla vztahovat na případy, kdy dochází opravdu k rozsáhlému a složitému zpracování s mnoha účely zpracování.[238] Jiní autoři zdůrazňují, že účelem výjimky by mělo být zohlednění specifické situace mikropodniků a malých a středních podniků (s méně než 250 zaměstnanci) v souladu s recitálem 13 GDPR, čili právě organizace a podniky s méně než 250 zaměstnanci by

235 MALIŠ, P. *GDPR - 3. díl: Vedení záznamů o činnostech zpracování osobních údajů*, op. cit.

236 *GDPR v kostce: praktický průvodce povinnostmi pro podniky a spolky*. Praha: C. H. Beck, 2018. ISBN 978-80-7400-704-0

237 Srov. ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 166 nebo KRÁL' Š. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobnic údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. op. cit. s. 249-250.

238 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 166.

např. jen proto, že vedou personální agendu, neměli být nuceni o takovém zpracování osobních údajů vést záznamy.[239]

Autorka se ztotožňuje s tím, že v praxi, dle striktního výkladu znění čl. 30 odst. 5 GDPR, by okruh správců či zpracovatelů, kterým by se mohla povinnost vést záznamy o činnostech zpracování v souladu s GDPR vyhnout, byl poměrně úzký, přičemž souhlasí s názory, že takové nastavení výjimek z povinnosti vést záznamy o činnostech zpracování zřejmě nebylo záměrem zákonodárce. Výslovné uvedení kritéria 250 zaměstnanců by naznačovalo, že právě na tyto subjekty by se výjimka v některých případech opravdu vztahovat měla.

Nicméně vzhledem k dosavadnímu v mnoha ohledech nejasnému výkladu čl. 30 odst. 5 GDPR, autorka považuje za vhodné, aby správci či zpracovatelé v případě, že si nebudou jistí, zda se na ně výjimka vztahuje, záznamy o činnostech zpracování z opatrnosti vždy vedli. Vedení záznamů o činnostech zpracování lze ostatně obecně považovat za praktické a užitečné z pohledu správce či zpracovatele, jelikož může být nápomocné v případě, kdy bude muset být dozorovému úřadu dokládán soulad prováděného zpracování s GDPR, případně i při výkonu práv subjektů údajů (zejména práva na přístup k osobním údajů a k informací dle čl. 15 GDPR). ÚOOÚ či někteří odborníci v oblasti ochrany osobních údajů, s ohledem na praktičnost záznamů o činnostech zpracování, také doporučují, aby tyto vedli i správci či zpracovatelé, kteří k tomu dle GDPR nemusí být nutně povinni.[240]

Pokud by některý správce nebo zpracovatel v praxi došel k závěru, že určitě není povinen vést záznamy o činnostech zpracování, měl by mít tento závěr v každém případě velmi důkladně podložený.

Do budoucna bude důležité sledovat, jakým způsobem budou výjimky z povinnosti vést záznamy o činnostech zpracování vykládány, ať už ze strany ÚOOÚ nebo Sboru.

4.2 Posouzení vlivu na ochranu osobních údajů

V případě, že správce zamýšlí provádět zpracování osobních údajů, které pravděpodobně bude mít za následek vysoké riziko pro práva a svobody fyzických osob, musí, dle čl. 35 odst. 1 GDPR, správce provést posouzení vlivu operací takového

239 KRÁL' Š. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobnic údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. op. cit. s. 250.

240 ÚOOÚ: *Základní příručka k GDPR*, 2. *Nové přístupy a povinnosti*. op. cit.

zpracování na ochranu osobních údajů, a to ještě před tím, než započne s prováděním zpracování. Již v první kapitole této práce bylo naznačeno, že povinnost provádět posouzení vlivu na ochranu osobních údajů je jednou z povinností, která je projevem přístupu založeného na riziku v pojetí dle GDPR. Jak je uvedeno výše v tomto odstavci, v čl. 35 odst. 1 GDPR je výslovně obsaženo, že posouzení vlivu na ochranu osobních údajů je nutné provádět pouze, pokud hrozí vysoké riziko pro práva a svobody fyzických osob. Povinnost provádět posouzení vlivu by se tedy neměla dotknout správců provádějících běžné nerizikové zpracování.

Na druhou stranu je ale nutné podotknout, že i když správci nevznikne povinnost provádět posouzení vlivu, protože jím zamýšlené zpracování nenaplní podmínky podle čl. 35 GDPR, správce musí pořád dbát o splnění obecné povinnosti průběžně zvládat a vyhodnocovat rizika při provádění zpracování, aby např. mohl určit, kdy se u konkrétního zpracování stane pravděpodobné, že bude pro subjekty představovat vysoké riziko ve smyslu čl. 35 odst. 1 GDPR.[241]

Lze se setkat i s názorem, že provedení posouzení vlivu na ochranu osobních údajů může být užitečné i pro některé správce, kteří k tomu dle čl. 35 GDPR nejsou povinni, a to zejména s ohledem na to, že např. z důvodu rychlého vývoje technologií se může stát, že zpracování, které aktuálně nepodléhá povinnosti provádět posouzení vlivu dle GDPR, této povinnosti v blízké době podléhat bude.[242] WP29 ostatně také vyzdvihuje užitečnost institutu posouzení vlivu na ochranu osobních údajů ve smyslu nástroje k zajištění a prokázání souladu zpracování s právními předpisy na ochranu osobních údajů (zejména s GDPR) dle čl. 24 odst. 1 GDPR, a doporučuje provedení posouzení vlivu vždy v případech, kdy si správce není jistý, zda se na něj povinnost dle 35 GDRP vztahuje nebo ne.[243]

WP29 jako záměr provádění posouzení vlivu označuje *popis zpracování údajů, posouzení jeho nezbytnosti a přiměřenosti a řízení rizik pro práva a svobody fyzických osob plynoucích ze zpracování osobních údajů, a to prostřednictvím jejich posouzení a stanovení opatření k jejich řešení*.[244]

241 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679* přijaté dne 4. 4. 2017, v aktualizovaném znění přijaté dne 4. 10. 2017.

242 YORDANOV, A. *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation, European Data Protection Law Review*, 4/2017, s. 491.

243 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, op. cit.

244 Tamtéž.

Povinnost provádění posouzení vlivu na ochranu údajů, dle názoru některých autorů, opět do určité míry nahrazuje oznamovací povinnost správce zakotvenou v § 16 ZOOÚ, která byla s účinností GDPR zrušena. Primárním účelem oznamovací povinnosti bylo, aby ÚOOÚ či jiné dozorové úřady členských států EU podchytily na základě plnění oznamovací povinnosti riziková zpracování osobních údajů[245], což se v zásadě ztotožňuje s účelem povinnosti provádět posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR a s tím související případné povinné konzultace s dozorovým úřadem podle čl. 36 GDPR.

4.2.1 Historie institutu posouzení vlivu na ochranu osobních údajů

Povinnost provádět posouzení vlivu na ochranu osobních údajů je další z povinností správců vyčtených v GDPR, která se oproti Směrnici 95/46/ES objevuje nově. V rámci celosvětového i evropského měřítka se ale o úplně neznámý institut nejedná. Evropská komise již v dílčích oblastech zdůrazňovala nutnost provedení posouzení dopadů na soukromí a ochranu osobních údajů správcem či zpracovatelem, a to konkrétně ve svém doporučení o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence (RFID) ze dne 12. 5. 2009 a v doporučení o přípravách na zavedení inteligentních měřicích systémů ze dne 9. 3. 2012. Na základě těchto doporučení Evropské komise pak WP29 vydala pokyny k posuzování vlivu na ochranu osobních údajů pro RFID aplikace a inteligentní měřicí systémy.[246]

V některých státech EU, nebo např. v Kanadě či USA, bylo provádění posouzení vlivu na ochranu osobních údajů (Privacy Impact Assessment - PIA) v určité formě známé a běžné i před účinností GDPR. Jako konkrétní příklad lze uvést Spojené království, kde bylo PIA již před účinností GDPR poměrně široce využíváno, a to zejména vládními, místními orgány, zdravotnickými organizacemi, ale též obchodními společnostmi. Spojené království bylo zároveň první zemí v Evropě, ve které došlo k vytvoření a zveřejnění PIA metodiky ze strany národního úřadu pro ochranu osobních

245 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 121.

246 BIEKER, F., FRIEDEWALD, M., HANSEN, M., OBERSTELLER, H., ROST, M. *A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation*. Springer International Publishing Switzerland 2016, s. 2.

údajů (Information Commissioner's Office – ICO), a to již v roce 2007.[247] Obdobně PIA před účinností GDPR fungovalo i v případě Francie.[248]

Na území ČR lze určitou podobnost s institutem posouzení vlivu na ochranu osobních údajů dle GDPR nalézt v § 13 odst. 3 ZOOÚ, podle kterého má každý správce či zpracovatel provádět posouzení rizik za účelem předejití neoprávněnému zpracování osobních údajů a jakémukoliv jinému zneužití osobních údajů. Tato povinnost byla do ZOOÚ doplněna s účinností od 1. 9. 2007 zákonem č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru.[249] Posuzování rizik ve smyslu § 13 odst. 3 ZOOÚ nicméně nemuselo být vyhotovováno v písemné podobě.[250] Lze proto polemizovat o tom, zda správci či zpracovatelé důsledně prováděli posuzování rizik dle § 13 odst. 3 ZOOÚ, když takové posouzení nemuselo být nikde zachyceno, tudíž ani ÚOOÚ při provádění kontroly reálně nemohl plnění takové povinnosti zhodnotit.

4.2.2 Předpoklady vzniku povinnosti provádět posouzení vlivu na ochranu osobních údajů

GDPR v čl. 35 odst. 1 jen velmi obecně stanoví, že vznik povinnosti provádět posouzení vlivu je podmíněn skutečností, že je *pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob*. Přímo v GDPR je dále obsažen demonstrativní výčet případů, kdy zpracování pravděpodobně bude znamenat vysoké riziko pro práva a svobody fyzických osob ve smyslu čl. 35 odst. 1 GDPR.[251]

Jako první je v tomto výčtu uvedeno *systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve*

247 Information Commissioner's Office: Privacy Impact Assessment Executive Summary. Dostupné na https://ico.org.uk/media/about-the-ico/consultations/2047/pia-executive-summary.pdf.

248 I francouzský úřad na ochranu osobních údajů (Commission Nationale de l'Informatique et des Libertés – CNIL) vytvořil metodiku pro provádění PIA. Srov. https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

249 NEŠPŮREK, R., ŠUCHMAN, J., JAROŠ, J. *GDPR: Kdy a jak posuzovat vliv zpracování na ochranu osobních údajů a kdy konzultovat dozorový orgán?* 9. 11. 2017. Dostupné na https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/gdpr-kdy-a-jak-posuzovat-vliv-zpracovani-na-ochranu-osobnich-udaju-a-kdy-konzultovat-dozorovy-organ.

250 Důvodová zpráva k zákonu č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru.

251 Čl. 35 odst. 3 GDPR.

vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad.[252] Vodítka k tomu, kdy je možné zpracování označit jako systematické a rozsáhlé, jsou blíže specifikována níže v této práci v kapitole týkající se pověřenců pro ochranu osobních údajů.

V čl. 35 odst. 3 písm. b) GDPR je jako další příklad zpracování, u něhož bude třeba provést posouzení vlivu na ochranu osobních údajů, uvedeno rozsáhlé zpracování, jehož předmětem jsou zvláštní kategorie osobních údajů nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů, což je předpokladem i pro povinné jmenování pověřence pro ochranu osobních údajů (pokud je zpracování těchto údajů hlavní činností správce)[253].

Jako poslední je v demonstrativním výčtu obsaženém v čl. 35 odst. 3 GDPR uvedeno rozsáhlé systematické monitorování veřejně přístupných prostorů.[254] Za veřejný prostor ve smyslu čl. 35 odst. 3 písm. c) GDPR by přitom patrně neměl být považován internet, dle názoru některých autorů se veřejným prostorem měl rozumět prostor, na kterém se může fyzicky shromažďovat relativně neurčitý a neomezený okruh lidí.[255] Vhodným příkladem zpracování spadající pod čl. 35 odst. 3 písm. c) GDPR tak bude jakékoliv kamerové sledování veřejných prostor (obchodní centrum, knihovna, nádraží apod.).

WP29 ve svých pokynech dále uvádí seznam devíti kritérií, která by měla být brána v potaz při vyhodnocování, zda správci vzniká povinnost provádět posouzení vlivu na ochranu osobních údajů dle GDPR. Tato kritéria v zásadě zpřesňují či rozvádí pojmy použité v souvislosti s podmínkami pro povinné provádění posouzení vlivu v čl. 35 odst. 1 a odst. 3 GDPR, nebo na jiných místech v GDPR. Kritéria uvedená v pokynech WP29 mohou současně posloužit dozorovým úřadům členských států EU jako vodítka při vytváření seznamů druhů operací zpracování, které podléhají, resp. nepodléhají povinnosti provádět posouzení vlivu na ochranu osobních údajů.[256]

Mezi kritéria, která mají být zvážena při posuzování, zda určité zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, WP29 řadí hodnocení nebo bodování (scoring) subjektů údajů včetně profilování, automatizované rozhodování s právními nebo obdobně vážnými důsledky, systematické monitorování

252 Čl. 35 odst. 3 písm. a) GDPR.
253 Srov. čl. 37 odst. 1 písm. c) GDPR.
254 Čl. 35 odst. 3 písm. c) GDPR.
255 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* op. cit. s. 318.
256 Čl. 35 odst. 4 a 5 GDPR.

subjektů údajů, zpracování zvláštních kategorií osobních údajů a dalších údajů, které jsou kvůli zvýšenému riziku pro práva a svobody jednotlivců považovány za citlivé, zpracování osobních údajů v rozsáhlém měřítku, přiřazování nebo slučování datových souborů, zpracování údajů o zranitelných subjektech (děti, zaměstnanci apod.), zpracování s využitím nové technologie či nového organizačního řešení, zpracování bránící subjektům údajů v uplatňování jejich práv nebo ve využívání určité služby či uzavření určité smlouvy.[257]

K využití těchto devíti kritérií WP29 dále poznamenává, že s rostoucím počtem kritérií, které předmětné zpracování naplňuje, roste i pravděpodobnost, že zpracování bude mít za následek vysoké riziko pro práva a svobody subjektů údajů. Obecně lze, dle WP29, za zpracování vyžadující vždy provedení posouzení vlivu považovat takové zpracování, které splňuje dvě ze jmenovaných kritérií. Výše uvedené ale nevylučuje, že v některých případech by mělo být posouzení vlivu provedeno, byť bude naplněno třeba jen jedno z uvedených kritérií.[258]

Kromě obecné formulace výše popsaných devíti kritérií WP29 uvádí také několik konkrétních příkladů zpracování, která by měla povinnosti provést posouzení vlivu podléhat, včetně uvedení odkazů na obecná kritéria, která tato konkrétní zpracování naplňují. Pro zaměstnavatele jako správce osobních údajů je důležité výslovné zmínění systematického monitorování zaměstnanců (včetně sledování aktivity zaměstnanců na internetu, monitorování pracovních stanic zaměstnanců apod.) jako zpracování, u kterého zpravidla posouzení vlivu na ochranu osobních údajů bude povinné, jelikož splňuje kritéria systematického monitorování a zpracování údajů zranitelných subjektů.[259]

4.2.2.1 Seznamy druhů operací zpracování podle čl. 35 odst. 4 GDPR

K vymezení, zda určité zpracování bude podléhat povinnosti provést posouzení vlivu na ochranu osobních údajů, resp. zda určité operace zpracování pravděpodobně povedou ke vzniku vysokého rizika pro práva a svobody fyzických osob, by měli přispět též dozorové úřady jednotlivých členských států EU. Dozorové úřady obligatorně vypracují a zveřejní seznamy druhů operací zpracování, které budou

257 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, op. cit.
258 Tamtéž.
259 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, op. cit.

předmětem posouzení vlivu.[260] Výše uvedené seznamy musí dozorové úřady předat Sboru, který k předloženým seznamům vydá v souladu s čl. 64 odst. 1 písm. a) svoje stanovisko. Jelikož v rámci Sboru bude docházet k diskuzi a vydávání stanovisek k seznamům operací dle čl. 35 odst. 4 GDPR sestavených dozorovými orgány všech členských států, lze předpokládat, že dojde alespoň k částečnému sjednocení těchto seznamů napříč EU.[261]

K dnešnímu dni lze říci, že dozorové úřady všech 28 členských států EU sestavily seznamy operací zpracování dle čl. 35 odst. 4 GDPR, předložily tyto Sboru a Sbor již ke všem těmto seznamům přijal a zveřejnil svoje stanovisko podle čl. 64 odst. 1 písm. a) GDPR.[262]

ÚOOÚ se při vytváření seznamu operací zpracování podléhajících povinnosti provést posouzení vlivu na ochranu osobních údajů vydal cestou nastavení obecných kritérií, při jejichž naplnění bude možné určité operace zpracování vyhodnotit jako vysoce rizikové, nikoliv cestou sestavení seznamu jednotlivých druhů operací zpracování, které by měly podléhat posouzení vlivu. S ohledem na zvolenou variantu sestavení seznamů dle čl. 35 odst. 4 GDPR ÚOOÚ zdůraznil, že bude nutné zároveň sestavit seznam operací zpracování nepodléhajících povinnosti provést posouzení vlivu, aby bylo zohledněno uplatňování výjimek pro některé druhy zpracování, které by jinak mohly být považovány jako vysoce rizikové (např. dle čl. 35 odst. 10 GDPR nebo recitálu 91 GDPR).[263]

ÚOOÚ při vytváření seznamu operací zpracování podléhajících povinnosti provést posouzení vlivu na ochranu osobních údajů vzal v potaz kritéria uvedená v pokynech WP29 k posouzení vlivu na ochranu osobních údajů a některá z nich v rámci svého seznamu dále rozpracoval a konkretizoval. Návrh seznamu operací zpracování dle čl. 35 odst. 4 GDPR odeslal Sboru ke stanovisku dne 1. 6. 2018.[264]

Dne 25. 9. 2018 Sbor přijal k seznamu operací podléhajících povinnosti provést posouzení vlivu na ochranu osobních údajů sestavenému ÚOOÚ stanovisko, ve kterém, v zájmu zajištění konzistentního výkladu podmínek pro provádění posouzení vlivu,

260 Čl. 35 odst. 4 GDPR.

261 *Vláda: ÚOOÚ: Stanovisko k povinnosti provádět posouzení vlivu na ochranu osobních údajů.* Právní rozhledy 13-14/2018, s. 3.

262 https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

263 Návrh dokumentů ÚOOÚ *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)*. Dostupné na https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385.

264 ÚOOÚ: Úřad k povinnosti provádět posouzení vlivu. Dostupné na https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385.

uvádí několik konkrétních připomínek a požadavků na úpravu seznamu ÚOOÚ. Sbor ve svém stanovisku např. doporučil, aby ÚOOÚ do seznamu dle čl. 35 odst. 4 GDPR explicitně uvedl, že je pouze demonstrativní. Dle názoru Sboru měl ÚOOÚ též doplnit seznam tak, aby byla patrná jeho návaznost a propojenost s pokyny WP29 k posouzení vlivu na ochranu osobních údajů (např. k jednotlivým druhům zpracování popsaných v seznamu uvést odkazy na konkrétní kritéria pro určení rizikovosti zpracování dle pokynů WP29 k posuzování vlivu na ochranu osobních údajů, ze kterých ÚOOÚ vycházel). Sbor měl také určité výhrady týkající se monitorování zaměstnanců, kdy Sbor doporučil, aby ÚOOÚ ve svém seznamu výslovně uvedl odkaz na dvě kritéria uvedená v pokynech WP k posouzení vlivu, která monitorování zaměstnanců splňuje (kritérium systematického monitorování a zpracování údajů zranitelných subjektů), aby bylo zcela zřejmé, že ÚOOÚ považuje systematické monitorování zaměstnanců jako zpracování podléhající povinnosti provést posouzení vlivu. Sbor dále např. uvedl, že předávání osobních údajů do zahraničí by obecně nemělo být důvodem pro vznik povinnosti provést posouzení vlivu na ochranu osobních údajů, a to jak samo o sobě, tak ve spojení s dalšími parametry, doporučil proto ÚOOÚ, aby ze svého seznamu odkazy na předávání osobních údajů do zahraničí úplně vyloučil.[265]

Připomínky Sboru uvedené v jeho stanovisku ÚOOÚ v zásadě všechny reflektoval[266] a dne 8. 2. 2019 ÚOOÚ zveřejnil dokument K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA) obsahující část označenou jako seznam druhů operací zpracování osobních údajů, které podléhají posouzení vlivu na ochranu osobních údajů, aktualizovaný v návaznosti na stanovisko Sboru.[267] Tento dokument ÚOOÚ tedy je možné považovat za oficiální seznam operací zpracování ve smyslu čl. 35 odst. 4 GDPR a správci by jej při vyhodnocování, zda se na ně vztahuje povinnost provádět posouzení vlivu na ochranu osobních údajů, měli zohlednit. Lze očekávat, že v budoucnosti bude tento seznam doplňován, a to zejména s ohledem na změny právních předpisů nebo rozvoj technologií.

265 *Opinion of the Board (Art. 64) 4/2018 on the draft list of the competent supervisory authority of Czech Republic regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*. Adopted on 25th September 2018. dostupné na https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

266 Pozn. autorky drobný nesoulad se stanoviskem Sboru lze spatřit v otázce vymezení pojmu zpracování ve „velkém rozsahu“, kdy Sbor doporučoval, aby ze seznamu operací zpracování sestaveného ÚOOÚ byla vypuštěna konkrétní čísla (např. od jakého počtu subjektů by zpracování mělo být považování za zpracování ve velkém rozsahu apod.). ÚOOÚ ve svém seznamu tato čísla ponechal s odůvodněním, že mají posloužit jako orientační pomůcka správcům (zvláště z ČR na území ČR) při analýze zpracování.

267 Dokument ÚOOÚ *K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA)*. Dostupný na https://www.uoou.cz/k-nbsp-povinnosti-spravcu-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju/d-33194.

Finální seznam druhů operací zpracování osobních údajů podléhajících posouzení vlivu na ochranu osobních údajů zpracovaný ÚOOÚ, obsahuje deset kritérií pro hodnocení rizikovosti zpracování odkazujících na kritéria WP29. U každého z těchto kritérií jsou vymezeny vždy tři stupně (skupiny) zpracování rozdělené podle míry rizika hrozícího pro práva a svobody fyzických osob (kritické hodnoty, významné hodnoty a nízké hodnoty). U každého takového stupně je uvedena vždy bližší charakteristika zpracování náležejícího do tohoto stupně, která by měla pomoci správci zařadit jím zamýšlené zpracování do správné skupiny. Správce může tedy k takovému seznamu operací zpracování přistupovat v podstatě jako k dotazníku, který vyplní tak, že podřadí zamýšlené zpracování pod jednotlivé stupně kritérií a následně provede dle vodítek ÚOOÚ analýzu, zda by se na něj měla vztahovat povinnost provést posouzení vlivu na ochranu osobních údajů.[268]

Autorka má za to, že seznam operací zpracování podléhajících posouzení vlivu na ochranu osobních údajů zveřejněný ÚOOÚ může v praxi napomoci správcům při analýze zpracování a hodnocení (ne)naplnění podmínek pro povinné provedení posouzení vlivu. Autorka kladně hodnotí vymezení stupňů v rámci jednotlivých kritérií. Tyto stupně, alespoň v některých případech, obsahují poměrně konkrétní a návodný popis zpracování, které by k nim mělo být přiřazeno, a pro správce by tak neměl být problém se v jednolitých kritériích orientovat. Na druhou stranu se však do určité míry stále jedná jen o obecný popis kritérií, která cílí na určité běžné typy zpracování, a v některých případech může být spolehlivé zařazování zpracování pod jednotlivá kritéria a jejich stupně komplikované. Opět je tak vhodné zdůraznit, že správci by stejně měli vždy zohledňovat veškerá specifika jím zamýšleného zpracování, a s přihlédnutím k těmto hodnotit rizikovost zpracování.

4.2.2.2 Výjimky z povinnosti provádět posouzení vlivu na ochranu osobních údajů

V GDPR a jím předvídaných dokumentech je také nastíněno, jaké zpracování naopak nebude podléhat povinnosti provádět posouzení vlivu na ochranu osobních údajů.

Prvním případem bude logicky situace, kdy není pravděpodobné, že zpracování s sebou ponese vysoké riziko pro práva a svobody fyzických osob. Na tomto místě je ale nutné upozornit, že správce by měl dbát na řádné zdůvodnění a ideálně i

268 Tamtéž.

zdokumentování toho, proč zpracování z různých důvodů nepodléhá povinnosti provést posouzení vlivu, a to zvláště v případě, kdy bude naplněno některé ze zmiňovaných kritérií uvedených v pokynech WP29 týkajících se posouzení vlivu.

Zároveň GDPR stanoví, že není nutné, aby správce pro obdobné operace zpracování, které představují podobné riziko, prováděl několik separátních posouzení pro ochranu osobních údajů. Naopak pro zpracování podobné co do jejich rozsahu, účelu, rizik s nimi spojených, postačí provedení jednoho posouzení vlivu.[269] Příznačným případem, kdy bude stačit jediné posouzení vlivu pro několik zpracování, jsou zpracování, která jsou prováděna za využití totožných nebo obdobných technologií, jejichž předmětem jsou stejné nebo velmi podobné druhy osobních údajů a jejichž účel je taktéž shodný. Jako konkrétní příklad pak lze uvést provozování videokamer na několika různých vlakových nádražích jediným provozovatelem vlakových nádraží (správcem).[270]

V čl. 35 odst. 10 GDPR je formulována další výjimka z povinnosti provést posouzení vlivu na ochranu osobních údajů, která se uplatní v případě zpracování majícího základ v právu EU nebo v právu členského státu vztahujícího se na daného správce, za předpokladu, že posouzení vlivu na ochranu osobních údajů bylo provedeno při přijímání předmětného právního předpisu a tento právní předpis upravuje konkrétní operace zpracování. Každý členský stát ale může stanovit, že i za situace, kdy má zpracování právní základ v určitém právním předpise splňujícím podmínky dle čl. 35 odst. 10 GDPR, je nutné posouzení vlivu na ochranu osobních údajů provést. Výjimku pro zpracování mající právní základ v právních předpisech jen velmi obecně a, dle názoru autorky, poněkud nadbytečně, opakuje i ZZOÚ.[271]

K výjimce podle čl. 35 odst. 10 GDPR nicméně WP29 podotýká, že před samotným započetím zpracování by správce zpracovávající osobní údaje na základě právního předpisu měl provést minimálně přezkum posouzení vlivu na ochranu osobních údajů provedeného při přijímání relevantního právního předpisu. V některých případech může být dokonce nutné, aby správce sám provedl kompletní posouzení vlivu

269 Čl. 35 odst. 1 věta druhá.

270 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679*, op. cit.

271 § 10 ZZOÚ stanoví, že *„Správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést.“*.

svého konkrétního zpracování na ochranu osobních údajů, byť se dané zpracování zakládá na právním předpise, při jehož přijímání již bylo posouzení vlivu provedeno.[272]

Důvodem pro provedení posouzení vlivu na ochranu osobních údajů správcem navzdory provedení „obecného" posouzení vlivu při přijímání právního předpisu může být např. skutečnost, že při posouzení vlivu na ochranu osobních údajů zákonodárce vycházel z určitého stavu technologií využívaných při zpracování osobních údajů, přičemž tyto se velmi rychle vyvíjejí, tudíž posouzení vlivu provedené před přijetím právního předpisu nemusí být po určité době aktuální. Navíc posouzení vlivu prováděné v souvislosti s přijímáním právního předpisu bude vždy do ve větší míře obecné a nikdy nebude moci postihnout všechna specifika zpracování prováděného konkrétními správci, která však mohou být z pohledu posouzení vlivu na ochranu osobních údajů podstatná. Lze se tak setkat s názorem, že i když je posouzení vlivu prováděné na úrovni legislativního procesu vítané, bude moci být považováno spíše jako obecné zastřešující posouzení vlivu pro daný typ operací zpracování s tím, že každý správce by pak měl provést svoje vlastní „zvláštní" posouzení vlivu zohledňující veškerá specifika při jím prováděném zpracování (např. zohlednění konkrétních využívaných technologií a s tím spojených rizik pro práva a svobody subjektů údajů). Toto „zvláštní" posouzení vlivu bude v ideálním případě do značné míry vycházet z obecného posouzení vlivu provedeného při přijímání předpisu, a mělo by být v důsledku toho z hlediska časového i finančního méně nákladné než „běžné" posouzení vlivu.[273]

Autorka se s názorem popsaným v předchozím odstavci ztotožňuje, a má za to, že i když by se na správce měla vztahovat výjimka z povinnosti provádět posouzení vlivu podle čl. 35 odst. 10 GDPR, měl by se z opatrnosti zaměřit na to, jakým způsobem bylo provedeno posouzení vlivu na úrovni legislativního procesu a zda bude pro jím zamýšlené zpracování, s ohledem na veškerá jeho specifika a použité technologie, dostačující. V případě potřeby by pak správce měl pro jistotu v podstatě doplnit a upřesnit obecné posouzení vlivu provedené na legislativní úrovni v návaznosti na specifika jím zamýšleného zpracování. Až rozhodovací praxe dozorových orgánů či soudů však ukáže, jakým způsobem bude přistupováno k aplikaci výjimky z povinnosti provádět posouzení vlivu na ochranu osobních údajů podle čl. 35 odst. 10 GDPR.

272 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, op. cit.

273 BIEKER, F., FRIEDEWALD, M., HANSEN, M., OBERSTELLER, H., ROST, M. *A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation*. op. cit., s. 5.

Dalším příkladem, kdy u zpracování nebude nutné provést posouzení vlivu na ochranu osobních údajů, je ten, kdy bude předmětné zpracování obsaženo v seznamu druhů operací zpracování, u nichž není třeba provádět posouzení vlivu na ochranu osobních údajů.[274] Dozorové úřady seznamy druhů operací zpracování podle čl. 35 odst. 5 GDPR sestaví a zveřejní dobrovolně. Pokud tak učiní, musí, stejně jako v případech seznamů druhů operací zpracování dle čl. 35 odst. 4 GDPR, tyto předat Sboru. Správce by při možném využití seznamů druhů zpracování podle čl. 35 odst. 5 GDPR vždy měl důkladně přezkoumat, zda jím zamýšlené operace zpracování skutečně odpovídají těm uvedeným v tomto seznamu.

ÚOOÚ již zveřejnil návrh demonstrativního seznamu operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů. V úvodu tohoto návrhu ÚOOÚ zdůrazňuje snahu minimalizovat administrativní zatížení menších a středních podniků, která by se měla promítat i v předloženém návrhu seznamů dle čl. 35 odst. 5 GDPR. K druhům operací zpracování, která by neměla podléhat posouzení vlivu na ochranu osobních údajů, ÚOOÚ řadí např. zpracování prováděné advokáty či notáři, jehož předmětem jsou osobní údaje klientů, které je nutné zpracovávat za účelem poskytování právních služeb (za splnění dalších podmínek)[275], pro zaměstnavatele je pak podstatné zařazení zpracování, které je plněno za účelem plnění zákonné povinnosti v oblasti vedení účetnictví, personální a mzdové agendy, sociálního a zdravotního pojištění.[276] Seznam operací zpracování dle čl. 35 odst. 5 sestavený ÚOOÚ se však nachází zatím ve fázi návrhu, dle vyjádření ÚOOÚ bude předložen Sboru ke stanovisku, a následně bude zveřejněna finální verze tohoto dokumentu.[277]

Závěrem je ke vzniku povinnosti provést posouzení vlivu na ochranu osobních údajů vhodné podotknout, že pokud správce provádí několik různých zpracování, je možné, že povinnost provádět posouzení vlivu na ochranu osobních údajů se na některé jím prováděné zpracování vztahovat bude a na jiné nikoliv. Pouhá skutečnost, že některé správcem zamýšlené zpracování podléhá povinnosti dle čl. 35 GDPR neznamená, že by správce nutně musel posouzení vlivu provádět i u všech ostatních „nerizikových“ zpracování.[278]

---

274 Čl. 35 odst. 5 GDPR.

275 Srov. recitál 91 GDPR.

276 ÚOOÚ: *Návrh seznamu operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů*. Dostupné na https://www.uoou.cz/dokumenty-k-gdpr/ds-4720/p1=4720.

277 Dokument ÚOOÚ *K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA)*. op. cit.

278 ŽŮREK, J. *Praktický průvodce GDPR*, op. cit. s. 122.

4.2.3 Proces provádění posouzení vlivu na ochranu osobních údajů

Jak plyne z čl. 35 odst. 1 věty první GDPR, posouzení vlivu by mělo být provedeno před zahájením zpracování, a to co nejdříve ve fázi přípravy zpracování. Proces posouzení vlivu na ochranu osobních údajů by přitom neměl být chápán jako jednorázový, ale naopak jako kontinuální proces, který provází celý životní cyklus určitého zpracování.[279] S pojetím posouzení vlivu na ochranu osobních údajů jako kontinuálního procesu souvisí též povinnost správce provádět pravidelně přezkum, zda je prováděné zpracování v souladu s posouzením vlivu na ochranu osobních údajů, a to alespoň v případě změn v rizicích, které představuje zpracování.[280] V návaznosti na tento přezkum pak, bude-li to nutné, správce provede aktualizaci nebo doplnění posouzení vlivu na ochranu osobních údajů provedené před zahájením zpracování.

Za zajištění řádného provedení posouzení vlivu na ochranu osobních údajů odpovídá vždy jen správce, byť reálně může posouzení vlivu provádět osoba odlišná od správce. V souladu s čl. 35 odst. 2 GDPR si při provádění posouzení vlivu správce musí k tomuto vyžádat posudek pověřence pro ochranu osobních údajů, byl-li daným správcem jmenován. Aby mohl pověřenec poskytovat adekvátní a včasné poradenství ohledně provádění posouzení vlivu na ochranu osobních údajů dle čl. 39 odst. 1 písm. c) GDPR a čl. 35 odst. 2 GDPR, měl by správce zajistit, že pověřenec bude do procesu posouzení vlivu zapojen po celou dobu jeho trvání, a bude tak mít přehled o všech dílčích částech tohoto procesu.[281] Další rolí pověřence v rámci procesu posouzení vlivu na ochranu osobních údajů je průběžné sledování uplatňování posouzení vlivu.[282]

Svoji úlohu v procesu posouzení vlivu na ochranu osobních údajů bude mít i zpracovatel, využívá-li jej správce pro provádění daného zpracování. Zpracovatel by měl být správci při provádění posouzení vlivu nápomocen a poskytnout mu potřebnou součinnost (zejména správci poskytnout všechny potřebné informace).[283]

Co se týče zapojení osob odlišných od správce do procesu posouzení vlivu na ochranu osobních údajů, je nutné zmínit ještě čl. 35 odst. 9 GDPR, který stanoví, že správce by si měl k jím zamýšlenému zpracování v rámci posouzení vlivu vyžádat stanovisko subjektů údajů nebo jejich zástupců. Stanovisko subjektů údajů by mělo být

279 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, op. cit.
280 Čl. 35 odst. 11 GDPR.
281 YORDANOV, A. *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation*, op. cit., s. 493.
282 Čl. 39 odst. 1 písm. c) GDPR.
283 Čl. 28 odst. 3 písm. f) GDPR.

dle téhož odstavce GDPR vyžadováno jen ve *„vhodných případech“*. V jakých konkrétních případech by stanovisko mělo být vyžadováno, resp. co se rozumí pojmem „ve vhodných případech“, GDPR dále nijak nespecifikuje. WP29 ve svých pokynech k posouzení vlivu na ochranu osobních údajů také nijak zvlášť neosvětluje, podle čeho by měl správce posuzovat, zda bude v jeho případě vhodné si stanovisko subjektů údajů vyžádat, nebo např. jaký okruh subjektů údajů by měl správce za účelem získání stanoviska oslovit, jaký počet subjektů bude dostačující pro získání stanoviska dle čl. 35 odst. 9 GDPR apod. WP29 se jen obecně vyjadřuje mj. ke způsobu získání stanoviska od subjektů údajů (kdy jako příklad uvádí položení relevantních otázek zástupcům zaměstnanců), nebo doporučuje, aby správce, nezíská-li stanovisko od subjektů, tuto skutečnost řádně odůvodnil a své odůvodnění zdokumentoval.[284]

Jelikož zatím neexistují žádné odpovídající podklady či poznatky z praxe, ze kterých by bylo možné dovodit, kdy by správci měli vyžadovat stanovisko subjektů údajů a kdy to nutné nebude, autorka považuje za vhodnější, aby se správce v zájmu zajištění co největšího souladu s GDPR v každém případě spíše pokusil získat stanovisko subjektů údajů, ledaže by měl vážné důvody pro neuplatňování tohoto postupu (zejména některé z důvodů uvedených přímo v čl. 35 odst. 9 GDPR nebo nastíněných WP29 v pokynech k posouzení vlivu na ochranu osobních údajů).

K obsahovým náležitostem a jednotlivým dílčím krokům, které tvoří proces posouzení vlivu na ochranu osobních údajů, autorka uvádí na tomto místě následující. Obecný proces posouzení vlivu na ochranu osobních údajů se, podle čl. 35 odst. 7 GDPR skládá z níže uvedených základních náležitostí. Po zhodnocení, že se na správce vztahuje povinnost provést posouzení vlivu na ochranu osobních údajů, případně po rozhodnutí, že posouzení vlivu provede dobrovolně, by měl správce na prvním místě systematicky popsat zamýšlené operace zpracování a účely zpracování. V dalším kroku by mělo být přistoupeno k posouzení nezbytnosti a přiměřenosti zamýšleného zpracování s ohledem na konkrétní účel nebo účely zpracování.

Dále by mělo dojít k provedení posouzení rizik pro práva a svobody subjektů údajů, což je jednou z nejdůležitějších součástí procesu posouzení vlivu na ochranu osobních údajů. V rámci tohoto kroku by subjekt provádějící posouzení vlivu zejména měl určit veškerá možná rizika hrozící v souvislosti se zpracováním právům a svobodám fyzických osob, dále by měl být v souladu s recitálem 84 GDPR zhodnocen

284 Pozn. autorky: Důvodem pro nezískání stanoviska subjektů údajů může být např. ohrožení obchodních, veřejných zájmů nebo bezpečnosti zpracování, případně též nepřiměřenost nebo neproveditelnost získání takového stanoviska.

původ, povahu, zvláštnosti a závažnost takových rizik, dále též v souladu s požadavky recitálu 90 GDPR vyhodnocena pravděpodobnost vzniku a závažnost všech vysokých rizik, přičemž by měly být vzaty v potaz povaha, rozsah, kontext, účely zpracování, jakož i zdroje rizik, v tomto kroku by také mělo být zhodnoceno, zda správce respektuje práva subjektů údajů, které jim GDPR přiznává.[285]

Poslední z obsahových náležitostí uvedených v čl. 35 odst. 7 GDPR je popis plánovaných opatření, která správce přijme za účelem zmírnění zjištěných rizik, a to *včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu* s GDPR. Do plánovaných opatření mohou být zahrnuta např. technická a organizační opatření přijatá správce podle čl. 25 GDPR, nebo technická a organizační opatření dle čl. 32 GDPR.[286]

Další důležitou náležitostí posouzení vlivu, byť v GDPR výslovně neuvedenou, je dokumentace procesu posouzení vlivu, jejíž význam tkví mj. nápomoci k plnění povinnosti správce prokázat soulad zpracování s GDPR dle čl. 24 GDPR. Dokumentace také poslouží správci jako podklad při výše zmiňovaném přezkumu souladu zpracování s posouzením vlivu na ochranu osobních údajů.[287]

V souvislosti s náležitostmi posouzení vlivu na ochranu osobních údajů požadovanými GDPR je vhodné zmínit čl. 35 odst. 8 GDPR, který stanoví, že správce by měl při posouzení vlivu na ochranu osobních údajů zohlednit i dodržování schválených kodexů chování podle čl. 40, což může být pro správce užitečné při prokazování, že zvolil adekvátní opatření ke zmírnění rizik zpracování.[288]

Náležitosti posouzení vlivu vyčtené v čl. 35 odst. 7 GDPR představují jen obecný rámec a obecné požadavky kladené na proces posouzení vlivu na ochranu osobních údajů. Stanovení přesné formy a struktury posouzení vlivu na ochranu osobních údajů je ponecháno na vůli správců, přičemž správce může využít různé metodiky, které byly již dříve vytvořeny dozorovými úřady členských států EU. Návrhy takových metodik jsou obsaženy v příloze č. 1 k pokynům WP29 k posouzení vlivu na

285 YORDANOV, A. *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation*, op. cit., s. 492.

286 Srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 320.

287 YORDANOV, A. *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation*, op. cit., s. 494. Dokumentace je jako dílčí krok procesu posouzení vlivu na ochranu osobních údajů obsažena též v *Pokynech WP29 pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679.*

288 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, op. cit.

ochranu osobních údajů a řadí se k nim např. *Conducting privacy impact assessments code of practice* vypracované britským ICO či, *Privacy Impact Assessment (PIA)* vydané francouzským CNIL nebo německý Standardní model pro ochranu osobních údajů. Správce má sice při výběru metodiky určitou volnost, musí ale vždy pamatovat na to, aby tato metodika odpovídala požadavkům na posouzení vlivu na ochranu osobních údajů stanoveným v GDPR. Za tímto účelem WP29 vypracovala přehled kritérií k prokázání, že určitá metodika všechny tyto požadavky splňuje.[289]

Další otázkou vyvstávající v souvislosti s procesem posouzení vlivu na ochranu osobních údajů je problematika zveřejnění posouzení vlivu na ochranu osobních údajů. GDPR správci neukládá povinnost posouzení vlivu zveřejnit, nicméně za účelem podpory důvěry ve zpracování prováděné správcem a za účelem zvýšení transparentnosti a prokázání odpovědnosti správce, WP29 obecně doporučuje posouzení vlivu na ochranu osobních údajů zveřejnit, a to alespoň část obsahující přehled nejdůležitějších závěrů.[290]

Na povinnost provádět posouzení vlivu na ochranu osobních údajů může v některých případech navazovat povinnost předchozí konzultace zpracování s dozorovým úřadem dle čl. 36 GDPR. Bude se jednat mj. o případy, kdy správce není schopen přijmout dostatečná opatření ke snížení rizik popsaných v posouzení vlivu na ochranu osobních údajů na přijatelnou míru, což znamená, že tzv. zbytkové riziko zůstane vysoké.[291]

4.3 Pověřenec pro ochranu osobních údajů

4.3.1 Vývoj institutu pověřence pro ochranu osobních údajů

Další povinností označovanou v souvislosti s účinností GDPR za novou, je povinnost správce a zpracovatele jmenovat, při naplnění podmínek dle čl. 37 GDPR, pověřence pro ochranu osobních údajů jakožto osobu, jejímž úkolem je zejména poskytovat správci či zpracovateli poradenství v oblasti ochrany osobních údajů, monitorovat soulad zpracování osobních údajů s právními předpisy či spolupracovat s dozorovým úřadem a být kontaktní osobou ve věci ochrany osobních údajů.[292]

289 Tamtéž.
290 Tamtéž.
291 WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, op. cit.
292 Čl. 39 odst. 1 GDPR.

Je však nutné zdůraznit, že ne ve všech členských státech je institut pověřence pro ochranu osobních údajů úplnou novinkou tak, jak je tomu v případě České republiky. V některých členských státech EU vnitrostátní právní úprava již před účinností GDPR zakotvila povinnost či možnost jmenovat nezávislého „pověřence pro ochranu osobních údajů“, což souvisí zejména s čl. 18 odst. 2 Směrnice 95/46/ES, ve kterém byla zakotvena možnost pro členské státy upravit institut osoby pověřené ochranou osobních údajů na vnitrostátní úrovni. WP29 ostatně již za účinnosti Směrnice 95/46/ES zdůrazňovala význam jmenování osob pověřených ochranou osobních údajů jakožto jednoho z konkrétních opatření, které může sloužit k naplnění obecné zásady odpovědnosti a k zajištění dodržování souladu zpracování osobních údajů s právními předpisy.[293] Tento závěr WP29 vyzdvihla a potvrdila i později v Pokynech týkajících se pověřenců pro ochranu osobních údajů přijatých před účinností GDPR.[294]

Příkladem členského státu EU, ve kterém byl institut nezávislého pověřence znám již před účinností GDPR, je Německo, kde bylo jmenování „pověřence pro ochranu osobních údajů“ po některých společnostech vyžadováno dokonce již před přijetím Směrnice 95/46/ES, a to od roku 1977. Právě německým modelem pověřence je inspirována úprava pověřence pro ochranu osobních údajů obsažená v čl. 37 a násl. GDPR.[295] S institutem pověřence před účinností GDPR operovaly v rámci EU také právní řády Francie, Maďarska, Slovinska či Polska.[296]

Nezávislého pověřence před účinností GDPR správci či zpracovatelé v mnoha členských státech jmenovali, kromě případů, kdy k tomu byli dle vnitrostátních právních předpisů povinni, jednoduše za účelem zajištění toho, že v rámci organizace bude existovat osoba, která se orientuje v oblasti ochrany osobních údajů a bude odpovědná za dodržování pravidel na ochranu osobních údajů, anebo z toho důvodu, že v daném členskému státě jmenování „pověřence na ochranu osobních údajů“ přinášelo správcům určité výhody (např. vynětí z povinnosti registrace/oznamovací povinnosti u místního dozorového orgánu, což předvídá čl. 18 odst. 2 Směrnice 95/46/ES).[297]

293 Stanovisko WP29 č. 3/2010 k zásadě *odpovědnosti* přijaté dne 13. července 2010.

294 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů* přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017.

295 VOIGT, P., *The compliance burden under the GDPR – Data Protection Officers*. Září 2016. Dostupné na https://globaldatahub.taylorwessing.com/article/the-compliance-burden-under-the-gdpr-data-protection-officers.

296 BOND, R., *The Role of the Data Protection Officer In Europe*. 6. 10. 2015. Dostupné na https://s3.amazonaws.com/documents.lexology.com/1373a119-14ae-4732-aed4-d9fbec519dc8.pdf.

297 DETLEV G., HICKMAN T., *Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation*. 13. 9. 2017. Dostupné na https://www.whitecase.com/publications/article/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data.

4.3.2 Jmenování pověřence pro ochranu osobních údajů

4.3.2.1 Povinné jmenování pověřence

Správce či zpracovatel je povinen, dle čl. 37 odst. 1 GDPR, jmenovat pověřence pro ochranu osobních údajů vždy, když je splněna alespoň jedna z následujících podmínek: zpracování je prováděno orgánem veřejné moci nebo veřejným subjektem (výjimku tvoří zpracování prováděné soudy při výkonu soudních pravomocí), hlavní činnosti správce či zpracovatele spočívají ve zpracování, které vyžaduje rozsáhlé, pravidelné a systematické monitorování subjektů údajů, nebo hlavní činnosti správce spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů dle čl. 9 GDPR a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů dle čl. 10 GDPR.

Vzhledem k tomu, že předpoklady, za nichž vzniká správcům či zpracovatelům povinnost jmenovat pověřence pro ochranu osobních údajů, jsou v GDPR definovány poměrně vágně, je vhodné se blíže věnovat jednotlivým pojmům použitým v definicích těchto podmínek pro povinné jmenování pověřence.

Jako první předpoklad, při jehož naplnění bude správce či zpracovatel povinen jmenovat pověřence, je ve výčtu v čl. 37 odst. 1 GDPR uveden případ, kdy je předmětné zpracování osobních údajů prováděno orgánem veřejné moci nebo veřejným subjektem. V GDPR přitom není objasněno, co se rozumí pojmy „orgán veřejné moci“ nebo „veřejný subjekt“. Dle názoru WP29, se kterým se autorka v zásadě ztotožňuje, by vymezení těchto pojmů totiž mělo být v dikci jednotlivých členských států.[298]

Z výše uvedeného plyne, že pojem „orgán veřejné moci“ a „veřejný subjekt“ je na našem území nutné vykládat v souladu s právními předpisy a judikaturou soudů ČR. Při výkladu pojmu „orgán veřejné moci“ lze vycházet z judikatury Ústavního soudu ČR, a to např. z nálezu Ústavního soudu ze dne 10. 11. 1998, sp. zn. I. ÚS 229/98.[299] Ústavní soud v tomto nálezu mj. odkazuje na názory přijaté již Ústavním soudem ČSFR, tedy, že pojmem veřejná moc se rozumí *moc, která autoritativně rozhoduje o právech a povinnostech subjektů, ať již přímo nebo zprostředkovaně*, přičemž veřejnou moc stát vykonává zejména *prostřednictvím orgánů moci zákonodárné, výkonné a soudní*. Pojem „orgán“ lze pak v právním slova smyslu vykládat jako právnickou osobu, která vykonává svoji činnost jako povinnost či kompetenci a která je zřízená k trvalému a

298 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
299 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*., 2018, op. cit. s. 243.

opakujícímu se výkonu činnosti. Typickým příkladem orgánu veřejné moci tak bude Poslanecká sněmovna a Senát Parlamentu ČR, ministerstva či soudy.

Co se týče pojmu „veřejný subjekt“, určité vodítko k výkladu tohoto pojmu poskytuje § 14 ZZOÚ, který stanoví, že povinnost jmenovat pověřence pro ochranu osobních údajů *mají kromě orgánů veřejné moci také orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu*. Účelem tohoto ustanovení má být, dle vyjádření Lubomíra Metnara, ministra vnitra, v podstatě konkretizace a zúžení pojmu „veřejný subjekt“ tak, aby pověřenec nemusel být jmenován v případech, kde by šlo o pouhou formalitu (jde např. knihovny, divadla apod.).[300] Lze tedy uzavřít, že pro účely posouzení povinnosti jmenovat pověřence by měl být za veřejný subjekt považován orgán (přesněji řečeno zřejmě právnická osoba) přímo zřízený zákonem plnící úkoly ve veřejném zájmu tímto zákonem vymezené.

Dle důvodové zprávy k § 14 ZZOÚ má povinnost jmenovat pověřence podle čl. 37 odst. 1 písm. a) dopadat na případy, kdy existuje formální i materiální nerovnováha mezi subjekty údajů a správcem,[301] ne však na případy, kdy by jmenování pověřence představovalo administrativní a finanční zátěž bez žádné přidané hodnoty (např. již zmiňovaná knihovna či divadlo zřízené jako příspěvková organizace obce). Kromě orgánů veřejné moci se má, dle důvodové zprávy, tato povinnost dotýkat subjektů, které se svoji povahou blíží orgánům veřejné moci (jako příklad je zde uvedena Česká národní banka, Nejvyšší kontrolní úřad, tedy subjekty, které plní veřejnoprávní funkce státu, ale nerozhodují nutně autoritativně o právech a povinnostech).

Čl. 37 odst. 1 písm. b) a c) GDPR ukládá správcům a zpracovatelům povinnost jmenovat pověřence v závislosti na obsahu jejich hlavní činnosti. Konkrétně pak stanoví povinnost pověřence jmenovat v případě, že hlavní činnost spočívá v operacích zpracování vyžadujících rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo v rozsáhlém zpracování zvláštních kategorií osobních údajů či údajů, které se týkají rozsudků v trestních věcech a trestných činů. Při výkladu těchto ustanovení je třeba se předně zaměřit na samotný pojem „hlavní činnost“. Určité upřesnění tohoto pojmu je obsaženo v recitálu 97 GDPR, který mj. stanoví, že hlavní činnosti správce

300 Zpravodajství Ministerstva vnitra ČR, Vitnerová M., *Vláda schválila návrh zákona o zpracování osobních údajů*. Dostupné na https://www.mvcr.cz/clanek/vlada-schvalila-navrh-zakona-o-zpracovani-osobnich-udaju.aspx.

301 Půjde např. o případ, kdy zákon, na základě kterého je správce plnící úkoly ve veřejném zájmu zřízen, stanovuje určitá omezení práv subjektů údajů. Příkladem takového správce je exekutorský či notářský úřad.

souvisejí se *základními činnostmi a nevztahují se na zpracování osobních údajů jakožto pomocnou činnost*. Jako hlavní činnost by přitom neměla být chápána výlučně vlastní (základní) činnost správce či zpracovatele spočívající ve zpracování osobních údajů, ale též operace zpracování osobních údajů, které jsou prováděny za účelem výkonu vlastní činnosti a jsou s tímto neoddělitelně spjaty.[302] Dobrým příkladem, na kterém je vysvětlen způsob, jakým by měl být chápán pojem „hlavní činnost", je nemocnice. Vlastní činností nemocnice je poskytování zdravotní péče pacientům. Avšak aby mohlo docházet k účinnému poskytování zdravotní péče, nemocnice musí zpracovávat osobní údaje pacientů, proto by zpracování takových údajů mělo být považováno za hlavní činnost nemocnice.[303]

Naopak zpracování osobních údajů, která jsou správci či zpracovateli prováděna jako podpůrná k hlavní činnosti, typicky půjde např. o vedení personální agendy, budou zpravidla považována za pomocné činnosti, nikoliv hlavní.[304] Logicky tedy pouhá skutečnost, že správce či zpracovatel vedle své vlastní činnosti systematicky zpracovává osobní údaje svých zaměstnanců, neznamená, že by měl mít povinnost jmenovat pověřence.

Další z předpokladů pro povinné jmenování pověřence podle čl. 37 odst. 1 písm. b) a c) GDPR je, že zpracování prováděné správcem či zpracovatelem je rozsáhlé. WP29 ve svém stanovisku uvádí několik kritérií, ke kterým by mělo být přihlíženo při hodnocení, zda je určité zpracování osobních údajů rozsáhlé či nikoliv. Těmito kritérii jsou počet dotčených subjektů údajů, objem údajů či škála různých údajových položek, které jsou zpracovávány, trvání či stálost zpracování, územní rozsah zpracování. Příkladem zpracování, které bude s největší pravděpodobností považováno za rozsáhlé, je zpracování osobních údajů zákazníků bankami při jejich obchodní činnosti, zpracování provozních, obsahových nebo lokalizačních dat poskytovateli telekomunikačních a internetových služeb, apod.[305]

Pokud zpracování osobních údajů představuje hlavní činnost správce či zpracovatele a je-li prováděné zpracování rozsáhlé, pak bude správce nebo zpracovatel povinen jmenovat pověřence, když zpracování představuje pravidelné a systematické monitorování subjektů údajů, nebo když jsou předmětem zpracování zvláštní kategorie údajů či údaje týkající se rozsudků v trestních věcech a trestných činů. Pojmu

302 ŽŮREK J. *Praktický průvodce GDPR*, op. cit. s. 113.
303 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
304 Tamtéž.
305 Tamtéž.

„pravidelné a systematické monitorování“ se opět věnuje WP29 ve svém stanovisku. Přímo GDPR tyto pojmy nijak blíže nedefinuje, byť v recitálu 24 GDPR zaměřeném na uplatňování GDPR v případech zpracování osobních údajů subjektů v EU ze strany správce či zpracovatele usazeného mimo EU, je operováno s pojmem „monitorování chování subjektů údajů“, které je zde chápáno ve smyslu sledování fyzických osob na internetu, včetně následného použití technik zpracování osobních údajů spočívajících v profilování. Jak však uvádí WP29, monitorování pro účely čl. 37 odst. 1 písm. b) GDPR nelze omezovat pouze na online prostředí, sledování v online prostředí by naopak mělo být považováno jenom za jeden z příkladů monitorování.[306] Dalšími příklady monitorování subjektů údajů může být sledování pohybu jejich mobilních telefonů či kamerové záznamy jejich pohybu.[307] Monitorování subjektů údajů je tak možné obecně definovat jako *každou aktivitu spočívající ve sledování subjektů údajů či jejich chování, a to bez ohledu na to, jestli k němu dochází fyzicky nebo v prostředí internetu.*[308]

Monitorování bude, dle WP29, pravidelné, pokud probíhá po určité období v určitých intervalech, nebo pokud se vyskytuje opakovaně, nebo se odehrává nepřetržitě či pravidelně. Pojem „systematické zpracování“ je pak vykládán jako zpracování, které je prováděné v souladu s určitým systémem, nebo je předem naplánované, organizované, nebo je součástí obecného plánu pro shromažďování údajů či součástí strategie správce nebo zpracovatele.[309]

Pravidelné a systematické monitorování lze tak zjednodušeně označit jako sledování subjektů údajů, které se nevyskytuje pouze náhodně, nýbrž opakovaně či dokonce nepřetržitě, a je určitým způsobem organizované, prováděné podle určitého systému.

Jako příklad pravidelného a systematického zpracování lze uvést cílení internetové reklamy pomocí e-mailu, provoz věrnostních programů pro zákazníky či sledování zdravotního stavu skrze „chytré“ náramky nebo hodinky.[310]

Posledním případem povinného jmenování pověřence je případ, kdy u správce či zpracovatele dochází ke zpracování zvláštních kategorií osobních údajů ve smyslu čl. 9

306 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
307 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*, op. cit. s. 252.
308 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* op. cit. s. 335.
309 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
310 OTEVŘEL P., *GDPR - 4. díl: Jste povinni jmenovat pověřence pro ochranu osobních údajů?* IT Systems č. 11/2017, dostupné na http://www.pravoit.cz/novinka/gdpr-4-dil-jste-povinni-jmenovat-poverence-pro-ochranu-osobnich-udaju.

GDPR nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů dle čl. 10 GDPR. V textu čl. 37 odst. 1 písm. c) je ne úplně vhodně použita spojka „a“ mezi dvěma výše uvedenými kategoriemi osobních údajů, nicméně WP29 poukazuje na skutečnost, že pro založení povinnosti jmenovat pověřence postačí, pokud správce či zpracovatel zpracovává osobní údaje náležející alespoň do jedné z uvedených kategorií. Znění čl. 37 odst. 1 písm. c) by, dle WP29, mělo být vykládáno se spojkou „nebo“.[311]

Nad rámec výše uvedených základních předpokladů, za kterých bude správce či zpracovatel povinen jmenovat pověřence pro ochranu osobních údajů, může členský stát dle čl. 37 odst. 4 GDPR stanovit i další případy, kdy správce nebo zpracovatel bude povinen pověřence jmenovat. Jak vyplývá z návrhu ZZOÚ i z důvodové zprávy k tomuto návrhu zákona, zákonodárce České republiky tuto možnost rozšířit případy, kdy bude jmenování pověřence povinné, nevyužil.

4.3.2.2 Dobrovolné jmenování pověřence

Zároveň platí, že nic nebrání tomu, aby správce či zpracovatel, který není povinen jmenovat pověřence dle čl. 37 odst. 1 GDPR, resp. dle vnitrostátní právní úpravy, jmenoval pověřence pro ochranu osobních údajů dobrovolně. Na takto jmenovaného pověřence se budou vztahovat ustanovení čl. 37 – 39 GDPR stejně jako kdyby se jednalo o případ povinného jmenování. Pokud by správce či zpracovatel měl zájem o zaměstnání osoby, jejíž náplní by byly úkoly v oblasti ochrany osobních údajů nebo o poskytování služeb v oblasti ochrany osobních údajů ze strany externisty, aniž by taková osoba byla pověřencem pro ochranu osobních údajů, je toto samozřejmě také možné. Bude třeba nicméně vždy, jak při komunikaci se subjekty údajů a s veřejností, tak v rámci styku s dozorovým orgánem, zřetelně uvést, že daná osoba není pověřencem pro ochranu osobních údajů ve smyslu GDPR.[312]

4.3.2.3 Jmenování jediného pověřence pro více subjektů

Čl. 37 odst. 2 GDPR umožňuje, aby skupina podniků jmenovala jen jednoho společného pověřence pro ochranu osobních údajů (tzv. skupinový pověřenec), který bude plnit úkoly pověřence ve vztahu ke všem členům skupiny, a to za předpokladu, že takto jmenovaný pověřenec bude snadno dosažitelný v každém podniku. Dosažitelnost pověřence přitom musí být zajištěna ve vztahu k subjektům údajů tak, aby se na něj subjekty údajů mohly snadno obracet dle čl. 38 odst. 4 GDPR, dále vůči dozorovému

311 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
312 *Tamtéž*.

úřadu, jelikož pověřenec působí jako kontaktní místo pro dozorový úřad podle čl. 39 odst. 1 písm. e) GDPR, ale i uvnitř dané organizace (podniku), neboť jedním z úkolů pověřence je i poskytování poradenství správcům, zpracovatelům a jejich zaměstnancům ohledně zpracování osobních údajů. Pro naplnění požadavku dosažitelnosti je třeba též pamatovat na čl. 37 odst. 7 GDPR, který ukládá správci a zpracovateli povinnost zveřejnit kontaktní údaje pověřence a sdělit tyto příslušnému dozorovému úřadu.[313]

Dosažitelnost nemusí nutně znamenat fyzickou přítomnost pověřence v podniku, ale i dostupnost prostřednictvím komunikačních prostředků na dálku. Důležitým aspektem dosažitelnosti je jazyková vybavenost společného pověřence, poněvadž pověřenec by měl být schopen účinně komunikovat a spolupracovat se subjekty údajů i dozorovými úřady v jazyce/jazycích používaných subjekty údajů a dozorovými úřady.[314]

Právě na požadavek na provádění komunikace v jazyce užívaném dotčenými subjekty údajů a dozorovými úřady mohou při snaze jmenovat společného pověřence narážet nadnárodní skupiny podniků. V takovém případě bude, dle názoru autorky, nejlepším řešením jmenování pověřence pro ty členy skupiny, kteří působí v určitém uceleném regionu spojeném stejným nebo podobným používaným jazykem, nacházejícím se ve stejném časovém pásmu, což bude v zásadě kopírovat i běžnou organizační strukturu nadnárodních korporací.[315] Požadavek jazykové vybavenosti nemusí být pro nadnárodní korporace nicméně takřka žádnou překážkou, pokud bude např. možné zajistit promptní překladatelské služby, nebo pokud pověřenec bude disponovat týmem odborníků, kteří se budou orientovat v prostředí konkrétních zemí/regionů a budou ovládat relevantní jazyky.

Podle čl. 37 odst. 3 platí, že jediný (společný) pověřenec může být jmenován také pro několik (různých) orgánů veřejné moci nebo veřejných subjektů s tím, že při úvaze o jmenování jediného pověřence musí být zohledněna vždy organizační struktura a velikost jednotlivých orgánů veřejné moci či veřejných subjektů. I v případě společného pověřence orgánů veřejné moci či veřejných subjektů bude nutné uplatňovat výše popsané kritérium dosažitelnosti, neboť bude předpokladem účinného plnění funkce pověřence.[316]

313 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
314 *Tamtéž.*
315 Srov. PATTYNOVÁ, J. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobníc údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. op. cit. s. 288.

4.3.3 Požadavky na osobu pověřence

Podle čl. 37 odst. 5 GDPR platí, že každý pověřenec *musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39*. Co je možné považovat za dostatečně vysokou úroveň profesních kvalit či odborných znalostí, není v GDPR blíže specifikováno, pouze v recitálu 97 GDPR je uvedeno, že by při hodnocení úrovně odborných znalostí mělo být přihlédnuto k prováděným operacím zpracování a k ochraně, která je vyžadována pro osobní údaje zpracovávané správcem nebo zpracovatelem. GDPR nestanoví ani žádné požadavky na úroveň dosaženého vzdělání pověřence. Každému správci nebo zpracovateli totiž může vyhovovat pověřenec s odlišnými profesními kvalitami a odbornými znalostmi či vzděláním (např. pro některého správce či zpracovatele budou klíčové znalosti a vzdělání v oblasti IT, pro jiného zase v oblasti práva). [317] Posuzování potřebných profesních kvalit a úrovně odborných znalostí tak bude individuální, a důležité bude, aby byl pověřenec jmenován vždy tak, že bude mít dostatečné profesní kvality a odborné znalosti k plnění úkolů pověřence u daného správce či zpracovatele.

Dle WP29 by správce či zpracovatel při posuzování odborných znalostí a profesních kvalit měl přihlížet vždy k citlivosti, složitosti a množství osobních údajů, které jsou zpracovávány, dále také např. k tomu, zda jsou osobní údaje (systematicky či příležitostně) předávány do zemí mimo EU. V každém případě by pověřenec měl mít dostatečné odborné znalosti v oblasti práva na ochranu osobních údajů, a to jak na úrovni EU, tak na národní úrovni, což by mělo zahrnovat i znalost praxe v oblasti ochrany osobních údajů na území EU i na vnitrostátní úrovni, což bude, dle autorky, zahrnovat i důkladnou znalost rozhodovací praxe národních dozorových úřadů, stanovisek a pokynů WP29, Sboru a národních dozorových úřadů či právních předpisů souvisejících s oblastí ochrany osobních údajů. Příhodná je též znalost organizace správce či zpracovatele s důrazem na znalost prováděných operací zpracování, informačních systémů využívaných správcem či zpracovatelem a potřeb v oblasti zabezpečení osobních údajů a dále znalost oboru, ve kterém správce nebo zpracovatel

316 Srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., 2017, *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 338 nebo PATTYNOVÁ J. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobnic údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. op. cit. s. 288.

317 *ÚOOÚ: Základní příručka k GDPR, 9. Pověřenec pro ochranu osobních údajů*. Dostupné na https://www.uoou.cz/9-poverenec-pro-ochranu-osobnich-udaju/d-27280.

podniká, v případě veřejného subjektu nebo orgánu veřejné moci i znalost správních předpisů vztahujících se na konkrétní orgán/subjekt.[318]

Vedle profesních kvalit a dostatečné úrovně odborných znalostí je pro osobu pověřence klíčové, aby byl schopen plnit úkoly, které pověřenci svěřuje GDPR. Za předpoklady schopnosti pověřence plnit své úkoly WP29 považuje osobní kvality (včetně profesní etiky a integrity), znalosti pověřenců i jejich postavení v rámci organizace.[319]

V praxi se objevují dotazy, jestli musí pověřenec disponovat certifikátem potvrzujícím jeho způsobilost vykonávat funkci pověřence. GDPR se problematikou certifikace pověřenců vůbec nezabývá, certifikát tedy není předpokladem pro to, aby konkrétní osoba mohla být jmenována pověřencem. Takový certifikát bude v zásadě jen prokazovat, že určitá osoba absolvovala odborný kurz pro pověřence pro ochranu osobních údajů.[320] Pokud se bude subjekt organizující takový odborný kurz jevit v očích správce či zpracovatele jako důvěryhodný, může být certifikát, dle názoru autorky, poměrně významným benefitem při volbě osoby pověřence ze strany správce nebo zpracovatele.

Autorka závěrem k požadavkům kladeným na osobu pověřence pro ochranu osobních údajů uvádí, že za nejvhodnějšího kandidáta na výkon funkce pověřence obecně považuje osobu s právnickým vzděláním, která se v praxi dlouhodoběji alespoň částečně zaměřuje na právo na ochranu osobních údajů, a tudíž získala komplexní znalosti v tomto oboru, a ideálně se též věnuje právu IT, případně má alespoň základní znalosti v oblasti IT, tedy je alespoň základě schopna se orientovat v systémech využívaných v souvislosti se zpracováním osobních údajů.

4.3.4 Interní a externí pověřenec

V souladu s čl. 37 odst. 6 platí, že pověřencem může být jmenován zaměstnanec správce či zpracovatele (interní pověřenec), nebo může pověřenec svoji funkci vykonávat na základě smlouvy o poskytování služeb (externí pověřenec pro ochranu osobních údajů). GDPR nevylučuje, aby služby pověřence pro ochranu osobních údajů zajišťovala pro správce či zpracovatele jako poskytovatel služeb též právnická osoba. I

318 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
319 *Tamtéž*.
320 ŽŮREK J. *Praktický průvodce GDPR*, op. cit. s. 120.

v tomto případě ale platí, že musí být označena konkrétní fyzická osoba, která zastává funkci pověřence.[321]

Obě varianty, tedy jmenování interního nebo externího pověřence, s sebou nesou určité výhody i nevýhody a správce či zpracovatel by měl vždy důsledně zvážit, zda pro něj bude vhodnější jmenování pověřence z řad zaměstnanců nebo využití služeb externisty.

Co se týče interního pověřence, je třeba v úvodu poukázat na skutečnost, že, byť se vztah mezi správcem či zpracovatelem a pověřencem bude řídit pracovní smlouvou, potažmo zákoníkem práce, pověřenec v několika ohledech není úplně běžným zaměstnancem. Zvláštnost postavení pověřence spočívá zejména v tom, že pověřenec v souladu s čl. 38 odst. 3 GDPR nesmí dostávat žádné pokyny týkající se výkonu jeho úkolů dle čl. 39 GDPR a zároveň platí, že nemůže být sankcionován ani propuštěn v souvislosti s plněním takových úkolů. Dle čl. 38 odst. 3 GDPR zároveň platí, že pověřenec má být v hierarchii správce či zpracovatele přímo podřízen vrcholovým řídícím pracovníkům.

Dle doporučení Ministerstva vnitra ČR obsaženém v metodických pokynech pro obce týkajících se funkce pověřence pro ochranu osobních údajů by pracovní poměr interního pověřence měl trvat po dobu neurčitou, nebo by pověřenec měl být jmenován na delší časové období za účelem seznámení se se všemi procesy relevantními pro zpracování prováděné správcem či zpracovatelem. Ministerstvo vnitra dále zdůrazňuje, že právní vztahy mezi interními pověřenci a správci či zpracovateli by neměly být založené dohodami o pracích konaných mimo pracovní poměr, a to z toho důvodu, že na dohody o pracích konaných mimo pracovní poměr se podle § 77 odst. 2 písm. g) zákoníku práce neaplikují ustanovení zákoníku práce o skončení pracovního poměru stanovená na ochranu zaměstnance.[322]

Výše uvedené závěry Ministerstva vnitra jsou sice formulovány „jen“ v rámci metodického doporučení k zabezpečení funkce pověřence adresovaného obcím, nicméně takové závěry lze, dle autorky, považovat za relevantní i pro účely ostatních správců a zpracovatelů, a to i s přihlédnutím k názoru WP29, že správci a zpracovatelé by měli vyvinout úsilí, aby smlouva uzavíraná mezi pověřencem a správcem či zpracovatelem obecně byla co nejvíce stabilní a obsahovala záruky proti

321 *ÚOOÚ: Základní příručka k GDPR, 9. Pověřenec pro ochranu osobních údajů*. op. cit.

322 *Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí podle právního stavu k 10. srpnu 2017*. Dostupné na https://www.mvcr.cz/clanek/zpravodajstvi-institut-poverence-pro-ochranu-osobnich-udaju-informace-pro-obce.aspx.

nespravedlivému propuštění pověřence, aby tak pověřenci mohli svoji funkci vykonávat co nejvíce nezávisle.[323]

Za jednu z hlavních výhod volby interního pověřence lze označit větší předpoklad znalosti organizace správce či zpracovatele, včetně znalosti interních procesů, informačních systémů, produktů a služeb. Obzvlášť v případě větších správců či zpracovatelů se složitější organizací by obeznámení se se všemi interními procesy, informačními systémy apod. nutnými pro řádné plnění úkolů pověřence mohlo být poměrně komplikované a časově náročné, a interní pověřenec tak pro takové správce či zpracovatele může být rozumnější volbou. Další typickou výhodou interního pověřence je obecně lepší dostupnost a jednodušší komunikace, zejména pracuje-li pověřenec ve stejné provozovně jako drtivá většina ostatních zaměstnanců správce.[324]

Nevýhody interního pověřence lze z pohledu správce a zpracovatele spatřovat ve větším riziku vzniku střetu zájmů (ve smyslu čl. 38 odst. 6 GDPR), dále v omezeních vyplývajících ze zákoníku práce (např. čerpání dovolené pověřencem, ochrana před ukončením pracovního poměru, limitace délky pracovní doby, náhrady škody způsobené zaměstnancem apod.).[325]

Druhou možností, jak může správce nebo zpracovatel zajistit výkon funkce pověřence, je uzavření smlouvy o poskytování služeb s externím subjektem. Externí pověřenec může být vhodnou variantou zejména pro střední či malé podniky, které nedisponují dostatečným počtem lidských zdrojů a/nebo finančních prostředků, aby zaměstnali interního pověřence, nebo pověřili některého ze stávajících zaměstnanců plněním úkolů pověřence.[326] U středních a menších podniků je také vyšší předpoklad, že jimi prováděné zpracování nebude nijak zvlášť rozsáhlé a komplikované, a tudíž nebudou potřebovat využívat služby pověřence v nijak zvlášť velkém rozsahu. V takovém případě je, dle názoru autorky, vhodnější uzavřít smlouvu s externím pověřencem, na základě které bude pověřenec k dispozici jen ve vymezeném rozsahu.

Smlouva, která bude uzavírána mezi správcem či zpracovatelem a externím pověřencem, případně právnickou osobou, která dodává pověřence, bude svoji povahou typicky smlouvou inominátní ve smyslu § 1746 odst. 2 OZ, případně též smlouvou příkazní řídící se § 2430 a násl. OZ. V každém případě by, vedle běžných náležitostí,

323 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
324 PATTYNOVÁ, J. in PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobníc údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. op. cit. s. 293.
325 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*, op. cit. s. 259-260.
326 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., 2017, *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 341.

které musí v souladu s OZ obsahovat smlouva, měla smlouva o poskytování služeb uzavíraná s pověřencem upravovat zejména i tyto záležitosti: výčet činností (úkolů), které bude pověřenec vykonávat, časový harmonogram poskytování služeb, určení výše ceny, nebo způsobu jejího určování, otázky spojené s možným střetem zájmů pověřence, zachování mlčenlivosti o skutečnostech, které se pověřenec dozví v souvislosti s plněním smlouvy (NDA), případně i označení osoby vykonávající funkci pověřence v případě uzavírání smlouvy s právnickou osobou, odpovědnost pověřence za škodu, dobu trvání smlouvy, způsoby a důvody pro ukončení smlouvy.[327]

Co se týče otázky ukončení smlouvy s externím pověřencem, je vhodné brát opět v potaz doporučení WP29, aby smlouva uzavíraná s pověřencem byla co nejvíce stabilní a obsahovala záruky proti nespravedlivému propuštění pověřence, tedy v ideálním případě stanovit delší dobu trvání smlouvy (nebo dokonce uzavřít smlouvu na dobu neurčitou), taxativně určit způsoby a důvody ukončení smlouvy a ostatní zákonné důvody a možnosti ukončení smlouvy vyloučit.

Výhodou externího pověřence je zajisté skutečnost, že se na vztah mezi ním a správcem či zpracovatelem nevztahují výše nastíněná omezení vyplývající ze zákoníku práce, tedy pověřenec i správce či zpracovatel mají větší volnost při sjednávání smlouvy o poskytování služeb, dále pak menší riziko vzniku střetu zájmů dle čl. 38 odst. 6 GDPR. [328]

Výhodou může být též lepší úroveň profesních kvalit a odborných znalostí, jelikož při volbě externího pověřence správce či zpracovatel zpravidla má na výběr mezi více různými experty, kteří mají zkušenosti v oblasti práva na ochranu osobních údajů, případně i IT a dalších relevantních oborech, nebo disponují odborným zázemím, které umožnuje propojování odborných znalostí ve všech relevantních oblastech a poskytování služeb pověřence skutečně komplexně a na vysoké úrovni (pověřencem může být jmenován např. advokát, který spolupracuje s dalšími advokáty majícími zkušenosti v oblasti práva na ochranu osobních údajů, práva IT, a tyto zkušenosti si navzájem předávají).[329] Výše uvedené odborné zázemí může být zároveň předpokladem

327 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*, op. cit. s. 265-266 a *Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí podle právního stavu k 10. srpnu 2017*. op. cit.

328 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*, op. cit. s. 260-261.

329 Srov. NEŠPŮREK, R., ŠUCHMAN J., JAROŠ J. *Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?* 26. 3. 2018. Dostupné na https://www.epravo.cz/top/clanky/poverenec-pro-osobni-udaje-dle-gdpr-kdy-koho-a-jak-poverit-107265.html nebo NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*., 2018, op. cit. s. 261.

snadné zastupitelnosti externího pověřence v době, kdy z různých důvodů není schopen plnit svoje úkoly.

Za hlavní nevýhody externího pověřence lze pak a contrario k výhodám interního pověřence označit potenciální nedostatek detailních znalostí o vnitřních záležitostech správce či zpracovatele, nedostatek bližšího kontaktu se zaměstnanci správce či zpracovatele, riziko horší dostupnosti pověřence, výjimečně i riziko střetu zájmů mezi různými klienty externího pověřence.[330]

Závěrem autorka uvádí, že zvláště ve větších korporacích provádějících rozsáhlejší zpracování osobních údajů, kde i před účinností GDPR nebylo výjimkou, že v rámci organizačního uspořádání existoval zaměstnanec nebo celé oddělení věnující se ochraně osobních údajů, považuje za logické, aby v případě potřeby nebo zájmu o jmenování pověřence došlo ke jmenování pověřence právě z řad těchto zaměstnanců. Samozřejmě za předpokladu, že bude možné zajistit naplnění podmínek kladených na pověřence GDPR (zejména zajištění nezávislosti pověřence ve smyslu čl. 38 odst. 3 GDPR, či vyloučení střetu zájmů dle čl. 38 odst. 6 GDPR).

Takoví zaměstnanci, kteří se v rámci organizace správce či zpracovatele již dříve intenzivně věnovali ochraně osobních údajů, by měli bez větších problémů splňovat jak požadavek orientace v organizaci a vnitřních procesech správce či zpracovatele, tak požadavek vysokých profesních kvalit a vysoké úrovně odborných znalostí. V případě, že správce či zpracovatel ke dni účinnosti GDPR neměl mezi svými zaměstnanci osobu, která by mohla adekvátně plnit úkoly pověřence, je otázkou, zda je rozumné se snažit doplnit kvalifikaci stávajícímu zaměstnanci, který nikdy předtím s oblastí ochrany osobních údajů v zásadě nepřišel do styku, a to absolvováním různých kurzů v oblasti GDPR, případně se snažit nalézt nového zaměstnance, který by roli pověřence byl schopen plnit, nebo se obrátit na externí subjekt poskytující služby pověřence na základě smlouvy o poskytování služeb.

Autorka je toho názoru, že zejména v prvních měsících a letech po účinnost GDPR nebude existovat příliš mnoho osob, které by disponovali přesvědčivou kvalifikací pro výkon funkce pověřence a byli by ochotní vykonávat funkci pověřence jako zaměstnanci správce či zpracovatele, proto autorka považuje ve většině případů za vhodnější obrátit se ve věci výkonu funkce pověřence na externí subjekty, které se

330 NAVRÁTIL, J. in NAVRÁTIL, J. a kol. *GDPR pro praxi*., 2018, op. cit. s. 261.

oblasti ochrany osobních údajů věnují dlouhodobě a jsou schopní pro správce nebo zpracovatele zajistit plnění odpovídajících úkolů pověřence.

4.3.5 Postavení pověřence

Postavení pověřence na ochranu osobních údajů se věnuje celý čl. 38 GDPR, který upravuje zejména otázky zajištění podpory, zdrojů a zapojení pověřence do všech potřebných procesů ze strany správce či zpracovatele, dále pak nezávislost a okrajově i odpovědnost pověřence za plnění svých úkolů, povinnost mlčenlivosti pověřence a zákaz střetu zájmů.

4.3.5.1 Zapojení pověřence do záležitostí souvisejících s ochranou osobních údajů

Na prvním místě, tedy v odst. 1 tohoto článku, GDPR stanoví, že pověřenec má být *náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů*. Správce či zpracovatel by tak měl zajistit, aby pověřenec byl informován a aby s ním správce či zpracovatel konzultoval zpracování osobních údajů od co nejranějšího stádia. Čím dříve totiž bude pověřenec informován o zamýšlených operacích zpracování osobních údajů a dalších záležitostech s tím spojených a bude se moci k těmto vyjadřovat, tím efektivněji bude pověřenec schopen plnit své úkoly, a tím spíše bude dosaženo souladu s GDPR.

V souvislosti s včasným zapojením pověřence do záležitostí souvisejících s ochranou osobních údajů je třeba poukázat na čl. 35 odst. 2 GDPR, který stanoví, že při provádění posouzení vlivu na ochranu osobních údajů před zahájením operací zpracování, si správce má vyžádat posudek pověřence pro ochranu osobních údajů. Což jenom potvrzuje a upřesňuje nutnost včasného zapojení pověřence.

WP29 poskytuje určitá vodítka k tomu, co by měl správce či zpracovatel zajistit, aby došlo k naplnění požadavku včasného a náležitého zapojení do záležitostí spojených s ochranou osobních údajů. Jedná se např. o vyzvání pověřence k účasti na schůzkách vedoucích pracovníků a středního managementu, zajištění přítomnosti pověřence při přijímání rozhodnutí s dopady na ochranu osobních údajů s tím, že pověřenci by včas měly být předány informace a podklady k tomuto rozhodnutí, aby mohl poskytnout relevantní posudek, dále by mělo být zajištěno, že jakékoliv stanovisko pověřence bude dostatečně zohledňováno a pokud správce či zpracovatel nebude souhlasit se stanoviskem pověřence, je vhodné zdokumentovat důvody tohoto nesouhlasu, WP29 též

doporučuje, aby si správce či zpracovatel vyžádal konzultaci s pověřencem, jakmile dojde k bezpečnostnímu incidentu.[331]

4.3.5.2 Poskytování podpory a zdrojů při plnění úkolů pověřence

Podle čl. 38 odst. 2 GDPR by správce či zpracovatel měli pověřenci poskytovat podporu při plnění jeho úkolů, tedy poskytovat pověřenci zdroje k plnění úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování odborných znalostí pověřence. Konkrétně lze pod podporu pověřence ze strany správce či zpracovatele podřadit mj. aktivní podporu ze strany vedoucích zaměstnanců správce či zpracovatele (např. poskytnutím rady), zajištění dostatečného času k plnění úkolů pověřence (tento aspekt bude hrát roli typicky v případě, kdy pověřenec plní kromě úkolů pověřence ještě jiné povinnosti), zajištění dostatečných finančních zdrojů, prostor, vybavení, případně týmu dalších pracovníků, stejně jako přístupu ke službám (IT, právní, bezpečnostní apod.), zajištění povědomí zaměstnanců správce či zpracovatele o tom, kdo byl jmenován pověřencem, zajištění vzdělávání pověřence (zejména průběžným školením). Rozsah podpory poskytované pověřenci je však třeba posuzovat s přihlédnutím k povaze správce či zpracovatele a zpracování osobních údajů, které provádí.[332]

4.3.5.3 Nezávislost, ochrana a odpovědnost pověřence

Velmi významný z hlediska postavení pověřence je čl. 38 odst. 3 GDPR, který v první větě stanoví, že pověřenec nemá dostávat žádné pokyny ve věci plnění svých úkolů, přičemž dodržování tohoto pravidla má zajistit správce či zpracovatel. Pověřenec by tedy neměl být v žádném případě nikým instruován, jak řešit určitou problematiku v oblasti ochrany osobních údajů, k jakému výsledku by mělo dospět řešení určitého problému, zda by se měl ohledně určité záležitosti obrátit na dozorový úřad s žádostí o konzultaci apod.[333] Výše uvedené by mělo značně přispět k tomu, aby byl pověřenec při plnění svých povinností nezávislý.[334]

Čl. 38 odst. 3 GDPR dále stanovuje pravidlo, dle kterého platí, že pověřenec nesmí být v souvislosti s plněním svých úkolů správcem nebo zpracovatelem propuštěn nebo sankcionován. Což má vést k posílení nezávislosti pověřence a k zajištění jeho ochrany zejména před tím, že by se pověřenci správce či zpracovatel chtěl „mstít“ kvůli

331 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
332 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
333 Tamtéž.
334 Recitál 97 GDPR mj. stanoví, že *pověřenci pro ochranu osobních údajů, bez ohledu na to, zda se jedná o zaměstnance správce, by měli být schopni plnit své povinnosti a úkoly nezávislým způsobem*.

plnění jeho úkolů.[335] Na straně pověřence by tak v žádném případě nemělo docházet k situacím, kdy by se bál správně plnit svoje úkoly dle GDPR (případně dle smlouvy) z důvodu, že určité jím poskytované rady a navrhované kroky mohou být z pohledu správce či zpracovatele „nepopulární“ (zejména protože mohou znamenat zvýšené finanční náklady).

Ustanovení zakazující správci či zpracovateli sankcionování pověřence v souvislosti s plněním jeho úkolů, dle názoru některých autorů, však nelze vykládat tak, že by správce nebo zpracovatel nemohl vůči pověřenci uplatnit nárok na náhradu škody způsobené pověřencem, neboť náhrada škody je institutem kompenzačním, nikoliv sankčním (represivním).[336] S tímto názorem se autorka ztotožňuje, neboť považuje za nepravděpodobné, že by úmyslem tvůrců GDPR bylo úplné vyloučení občanskoprávní či pracovněprávní odpovědnosti pověřence za škodu způsobenou správci či zpracovateli v souvislosti s nesprávným plněním jeho úkolů.

Výše uvedený závěr v zásadě potvrzuje i současné pojetí občanskoprávní, resp. pracovněprávní odpovědnost, kdy u obou je zdůrazňována zejména její preventivní funkce (tj. předcházení škodám, působení na subjekty, aby jednali tak, že budou dodržovat právní předpisy a předcházet škodám) a reparační funkce (odčinění vzniklé újmy). Funkce sankční (represivní) pro občanskoprávní potažmo pracovněprávní odpovědnost není typická.[337]

Autorka má proto za to, že pakliže dojde k naplnění předpokladů vzniku občanskoprávní odpovědnosti, tedy k protiprávnímu jednání (pověřenec poruší svoji povinnost plnit úkoly jemu svěřené), vzniku újmy (např. správce uhradí dozorovému úřadu pokutu, která mu byla uložena proto, že se řídil chybnou radou pověřence), příčinné souvislosti mezi protiprávním jednáním a vznikem újmy a zpravidla i k zavinění (ve formě úmyslu nebo nedbalosti)[338], vznikne na straně pověřence občanskoprávní odpovědnost a správce či zpracovatel bude oprávněn požadovat náhradu vzniklé škody.

335 ŽŮREK J. *Praktický průvodce GDPR*, op. cit. s. 118.

336 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 345.

337 ŠVESTKA, J. in DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M. a kol. *Občanské právo hmotné. Svazek 1. Díl první: Obecná část.* Praha: Wolters Kluwer ČR, s. 357-359. ISBN 978-80-7478-325-8 a BĚLINA M. in BĚLINA, M., PICHRT, J. a kol. *Pracovní právo. 7. doplněné a podstatně přepracované vydání*. Praha: C. H. Beck, 2017, s. 316. ISBN 978-80-7400-667-8.

338 ŠVESTKA, J. in DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M. a kol. *Občanské právo hmotné. Svazek 1. Díl první: Obecná část.* op. cit. s. 356.

U interního pověřence bude třeba zohlednit pravidla týkající se pracovněprávní odpovědnosti za škodu. Předpoklady vzniku obecné odpovědnosti zaměstnance za škodu vychází z předpokladů vzniku občanskoprávní odpovědnosti, a jsou následující: porušení pracovních povinností zaměstnancem při plnění pracovních úkolů nebo v přímé souvislosti s tím, vznik škody, kauzální nexus mezi porušením pracovních povinností a vznikem škody a zavinění na straně zaměstnance.[339] Při naplnění těchto požadavků vznikne zaměstnanci povinnost nahradit zaměstnavateli škodu v penězích (neodčiní-li zaměstnanec škodu uvedením v předešlý stav).[340] Je však třeba vzít v potaz § 257 odst. 2 zákoníku práce, který limituje výši náhrady škody způsobené zaměstnancem z nedbalosti částkou *rovnající se čtyřapůlnásobku jeho průměrného měsíčního výdělku před porušením povinnosti, kterým způsobil škodu*. Toto omezení se ale neuplatní, pokud zaměstnanec škodu způsobí úmyslně, v opilosti či po užití jiných návykových látek.

V souvislosti s možným vznikem odpovědnosti pověřence za škodu způsobenou správci či zpracovateli je vhodné podotknout, že za soulad s GDPR a dalšími právními předpisy na ochranu osobních údajů a schopnost doložit tento soulad samozřejmě dle čl. 5 odst. 2 GDPR odpovídá správce či zpracovatel, nikoliv pověřenec. Pokud správce nebo zpracovatel přijme určité rozhodnutí, které nebude odpovídat závěrům učiněným pověřencem, pověřenec by měl mít šanci svoje závěry dostatečně vyjasnit přímo vedoucím (rozhodujícím) pracovníkům správce nebo zpracovatele s čímž také souvisí znění věty třetí čl. 38 odst. 3 GDPR, která určí, že pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele.[341]

4.3.5.4 Kontaktní místo pro subjekty údajů

Dalším z důležitých aspektů postavení pověřence zakotvených v čl. 38 GDPR je působení pověřence jako kontaktního místa pro subjekty údajů, kteří se na pověřence mohou obracet ve všech záležitostech týkajících se zpracování jejich osobních údajů a výkonem jejich práv podle GDPR.[342]

339 NOVOTNÝ Z. in BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář. 2. vydání*. op. cit. s. 1022.
340 § 257 odst. 1 zákoníku práce.
341 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.
342 Čl. 38 odst. 4 GDPR.

4.3.5.5 Povinnost mlčenlivosti pověřence

Podle čl. 38 odst. 5 GDPR je pověřenec ohledně plnění svých úkolů vázán mlčenlivostí v souladu s právem EU nebo členského státu. Povinnost mlčenlivosti pověřence by měla zahrnovat obecnou povinnost zdržet se veškerého jednání, v důsledku kterého by mohlo dojít k předání informací, které pověřenec získal v souvislosti s plněním svých úkolů, neoprávněné osobě.

Mlčenlivost by se přitom neměla vztahovat jen na osobní údaje jako takové, ale i na bezpečnostní opatření, či jiné důvěrné informace, se kterými se při plnění úkolů pověřenec seznámí (např. i obchodní tajemství). V případě porušení povinnosti mlčenlivosti bude pověřenec odpovídat za škodu tímto způsobenou. Vyloučit nelze ani trestněprávní odpovědnost, když ze strany pověřence teoreticky může dojít k naplnění skutkové podstaty neoprávněného nakládání s osobními údaji podle § 180 zákona č. 40/2009 Sb., trestní zákoník, v účinném znění.[343] V každém případě lze předpokládat, že povinnost mlčenlivosti bude, jak již bylo uvedeno výše v této práci, poměrně detailně upravena vždy v pracovní smlouvě, nebo smlouvě o poskytování služeb uzavírané mezi pověřencem a správcem či zpracovatelem.

4.3.5.6 Střet zájmů

Při volbě osoby pověřence by správce či zpracovatel měl také pamatovat na to, že pověřenec sice pro správce nebo zpracovatele může, nad rámec výkonu funkce pověřence, plnit i další úkoly a povinnosti, plnění takových dalších povinností a úkolů však nesmí nikdy vést ke vzniku střetu zájmů, tedy ohrožení nezávislosti pověřence. Je na správci či zpracovateli, aby přijal taková opatření, v důsledku kterých bude riziko střetu zájmů eliminováno.[344]

Podle WP29 by správce či zpracovatel měl za účelem zamezení vzniku střetu zájmů zejména zajistit, že pověřenec nebude zastávat pozici, jejíž náplní by bylo určování účelů a prostředků zpracování osobních údajů. WP29 též ve svých pokynech uvádí konkrétní příklady pozic v rámci organizace správce či zpracovatele, u kterých je riziko vzniku střetu zájmů zvláště vysoké. Jedná se zejména o pozice vedoucích pracovníků (generální ředitel, finanční ředitel, vedoucí marketingového oddělení, vedoucí HR oddělení, nebo IT oddělení aj.), ale i další pozice, které mohou být

343 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 347.
344 Čl. 38 odst. 6 GDPR.

v hierarchii správce či zpracovatele níže, nicméně výkon těchto pozic vede k určování účelů a prostředků zpracování.[345]

Konkrétním příkladem, kdy snadno může dojít ke vzniku střetu zájmů tak může být pověření totožné osoby správou IT systémů (či vedením IT oddělení) a zároveň výkonem funkce pověřence, což by pravděpodobně vyústilo v situaci, kdy by pověřenec kontroloval sám sebe, zda vykonává činnosti spadající pod pozici IT managera v souladu s předpisy na ochranu osobních údajů.[346] Jako další lze uvést případ, kdy právník (typicky advokát) má vykonávat funkci pověřence a zároveň zastupovat správce či zpracovatele před soudy nebo jinými orgány ve sporech souvisejících s ochranou osobních údajů.[347]

Za účelem prevence střetu zájmů je správci či zpracovateli, s ohledem na jeho strukturu, velikost a vykonávané činnosti, doporučeno přijetí několika opatření. Tato opatření je vhodné přijmout, jak v případě, kdy u správce či zpracovatele bude fungovat interní pověřenec, tak v případě jmenování externího pověřence s tím, že je třeba přihlédnout k rozdílům, které plynou zejména z povahy smluvního vztahu. Primárně by správce či zpracovatel měl určit pozice, které jsou s funkcí pověřence neslučitelné (správci či zpracovatelé se orientačně budou moci řídit demonstrativním výčtem pozic uvedených v předchozím odstavci této práce), dále by mělo dojít k vypracování vnitřního předpisu, který vysvětlí, co se rozumí střetem zájmů a stanoví pravidla pro zamezení střetu zájmů. Správce či zpracovatel by měl také zajistit, aby v případě hledání uchazečů na pozici pověřence, bylo v nabídce této pracovní pozice uvedeno, co může způsobit vznik střetu zájmů. Obdobně i při jednání o smlouvě o poskytování služeb s externím pověřencem by měl kladen důraz na přesnou a dostatečnou formulaci pravidel pro předejití střetu zájmů.[348]

345 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.

346 K tomuto závěru dospěl už v minulosti dozorový úřad Bavorska (BayLDA), kde byla funkce pověřence zakotvena už před účinností GDPR. Společnosti, která jmenovala pověřencem osobu zastávající současně pozici IT managera, uložil tento úřad z důvodu vzniku střetu zájmů sankci. Srov. KAUFMANN J., GUENTHER J. *Germany: Data Protection Officer must not have a conflict of interests*. 21. 11. 2016. Dostupné na https://globalcompliancenews.com/germany-data-protection-officer-conflict-of-interest-20161121/.

347 K tomuto závěru opět v minulosti dospěl dozorový úřad Bavorska (BayLDA). Uvedený závěr ohledně střetu zájmů při výkonu funkce pověřence a právníka tento úřad aplikuje jak na členy interního právního oddělení, tak na externí subjekty poskytující právní služby. Srov. KAUFMANN J., GUENTHER J. *Data Protection Officers Must Not Have a Conflict of Interest – Part 2*. 9. 1. 2018. Dostupné na https://globalcompliancenews.com/data-protection-officers-conflict-interest-20180109/. Stejný názor, avšak jen ve vztahu k externím poskytovatelům právních služeb, prezentuje i WP29 v *Pokynech týkajících se pověřenců pro ochranu osobních údajů*.

348 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.

Jak již bylo naznačeno výše v této práci, riziko střetu zájmů je obecně vyšší v případě interních pověřenců, jelikož je z logiky věci pravděpodobnější, že správce či zpracovatel jako zaměstnavatel bude chtít pověřenci svěřit plnění dalších úkolů v rámci své organizační struktury. I v případě externího pověřence ale střet zájmů není vyloučen.

Ke střetu zájmů u externího pověřence může, obdobně jako u pověřence interního, dojít za situace, kdy správce či zpracovatel outsourcuje subjekt vykonávající funkci externího pověřence i na výkon jiné pozice, která je riziková z hlediska střetu zájmů (opět odkazuji na demonstrativní výčet pozic uvedený výše v této kapitole), což by de facto mohlo znamenat, že by pověřenec v rámci plnění svých úkolů kontroloval sám sebe při vykonávání činností spadajících do jiné jím zastávané pozice.[349]

4.3.6 Úkoly pověřence

Rozsah úkolů, které je pověřenec povinen plnit, je uveden v čl. 39 GDPR. Jak vyplývá ze znění čl. 39 GDPR, jedná se o výčet demonstrativní, a správce či zpracovatel může pověřenci uložit též plnění dalších úkolů (např. vytvoření záznamů o činnostech zpracování ve smyslu čl. 30 GDPR). Při ukládání takových dalších úkolů musí ale správce a zpracovatel brát vždy v potaz to, zda bude pověřenec schopen v odpovídající kvalitě plnit i úkoly nad rámec výčtu uvedeném v čl. 39 GDPR a zda nemůže plnění takových dodatečných úkolů vést ke vzniku střetu zájmů.[350]

Při plnění svých úkolů by se měl pověřenec obecně řídit zásadou uvedenou v čl. 39 odst. 2 GDPR, měl by tedy brát *patřičný ohled na riziko spojené s operacemi zpracování* a zároveň přihlížet *k povaze, rozsahu, kontextu a účelům zpracování* (přístup založený na riziku). V praxi to znamená, že pověřenec by si před tím, než začne s plněním úkolů, měl vytyčit priority, a to dle toho, které otázky zpracování osobních údajů považuje za rizikovější. Přednostně by se tak měl pověřenec věnovat oblastem, které z hlediska ochrany osobních údajů představují největší riziko.[351]

349 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 346.
350 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 348.
351 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.

4.3.6.1 Poskytování informací a poradenství

Jako první je v demonstrativním výčtu úkolů pověřence v čl. 39 odst. 1 GDPR uvedeno poskytování informací a poradenství v oblasti právních předpisů na ochranu osobních údajů na úrovni EU i vnitrostátní, a to přímo správcům a zpracovatelům, nebo jejich zaměstnancům, kteří provádí zpracování osobních údajů.

Jak již bylo uvedeno v kapitole této práce věnující se požadavkům na osobu pověřence, pověřenec by se měl orientovat v právních předpisech na ochranu osobních údajů, jakož i v praxi související s jejich aplikací, a měl by tak být schopen výše uvedeným subjektům poskytovat kvalifikované rady v dané oblasti a předávat těmto svoje znalosti (např. formou školení, vytvářením různých metodik/návodů apod.).[352]

4.3.6.2 Monitorování souladu s předpisy v oblasti ochrany osobních údajů

Dalším důležitým úkolem pověřence je monitorování souladu činností správce či zpracovatele s GDPR a dalšími právními předpisy v oblasti ochrany osobních údajů na úrovni EU i členských států.[353]

WP29 doporučuje, aby v rámci plnění povinnosti monitorování souladu, pověřenci průběžně shromažďovali informace pro identifikaci procesů zpracování, kontrolovali a vyhodnocovali soulad operací zpracování a o zjištěném souladu či nesouladu operací zpracování s předpisy na ochranu osobních údajů správce nebo zpracovatele informovali a vydávali doporučení. Odpovědnost za soulad s GDPR a dalšími předpisy na ochranu osobních údajů má nicméně v souladu s čl. 24 odst. 1 GDPR vždy správce, nikoliv pověřenec.[354] Pověřenec je oprávněn poskytovat správci toliko rady a doporučení ve věci souladu činností zpracování s právními předpisy, kterými se správce v konečném důsledku nemusí řídit.[355]

4.3.6.3 Poskytování poradenství ve věci posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování

V souladu s čl. 35 odst. 1 GDPR je provádění posouzení vlivu na ochranu osobních údajů povinností správce, nikoliv pověřence. Pověřenec nicméně zpravidla bude správci při provádění posouzení vlivu na ochranu osobních údajů poskytovat

352 NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. op. cit. s. 348 - 349.
353 Čl. 39 odst. 1 písm. b) GDPR.
354 Čl. 24 odst. 1 GPPR mj. stanoví, že *správce* (zavede) *vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením*.
355 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.

součinnost, a může mít v tomto procesu významnou roli.[356] Podle čl. 39 odst. 1 písm. c) GDPR je povinností pověřence poskytovat správci poradenství ohledně posouzení vlivu na ochranu osobních údajů, a to na základě žádosti správce, a monitorovat uplatňování posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR. S tímto ustanovením koresponduje čl. 35 odst. 2 GDPR, který ukládá správci povinnost vyžádat si posudek pověřence (pokud byl jmenován) při provádění posouzení vlivu na ochranu osobních údajů.

Dle doporučení WP29 by si správce v souladu s čl. 35 odst. 2 GDPR měl u pověřence vyžádat posudek k níže uvedeným otázkám. Nejdříve by měl správce pověřence požádat o stanovisko, zda je vůbec nutné/vhodné provádět posouzení vlivu na ochranu osobních údajů, pokud pověřenec dospěje k názoru, že by posouzení vlivu mělo být provedeno a správce se rozhodne pro jeho provedení, měl by si správce vyžádat posudek k tomu, jakou metodiku zvolit pro provádění posouzení vlivu, dále též k tomu, jestli bude vhodnější provedení posouzení vlivu interně nebo externě, jaká opatření by měla být uplatněna, aby došlo ke zmírnění rizik pro subjekty údajů, jakož i posudek, který komplexně zhodnotí provedené posouzení vlivu z hlediska jeho správnosti, včetně zhodnocení závěrů posouzení vlivu (tedy zda je v souladu s GDPR).[357]

Pokud by správce s kterýmkoliv z posudků poskytnutých pověřencem nesouhlasil, nemusí se jím nutně řídit, v tomto případě by však měl být v dokumentaci k posouzení vlivu na ochranu osobních údajů nesouhlas s posudkem pověřence výslovně uveden, včetně uvedení argumentů, proč s posudkem správcem nesouhlasí a proč tento posudek v souvislosti s prováděním posouzení vlivu nevezme v potaz.[358]

4.3.6.4 Spolupráce pověřence s dozorovým úřadem a působení jako kontaktní místo pro dozorový úřad

Posledními úkoly pověřence zahrnutými do demonstrativního výčtu v čl. 39 odst. 1 GDPR jsou *spolupráce s dozorovým úřadem* a *působení* (pověřence) *jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně*

356 V *Pokynech pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679WP29* přijatých dne 4. 4. 2017, v aktualizovaném znění přijatých dne 4. 10. 2017, WP29 uvádí, že posouzení vlivu na ochranu osobních údajů provádí *správce společně s pověřencem pro ochranu osobních údajů a zpracovateli*.

357 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.

358 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.

předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci.[359]

Úkoly stanovené v čl. 39 odst. 1 písm. d) a e) vychází zejména z role pověřence jako „zprostředkovatele“ mezi dozorovým úřadem (tedy ÚOOÚ) a správcem či zpracovatelem. Pověřenec jakožto kontaktní místo do určité míry usnadňuje dozorovému úřadu plnění jeho úkolů dle čl. 57 GDPR a výkon pravomocí podle čl. 58 GDPR (pověřenec zejména usnadňuje přístup dozorového úřadu k potřebným dokumentům a informacím).[360]

Jak již bylo zmíněno v kapitole věnující se jmenování pověřence, aby mohlo být působení jako kontaktní místo účinně provozováno, musí správce či zpracovatel podle čl. 37 odst. 7 GDPR sdělit dozorovému úřadu kontaktní údaje pověřence. ÚOOÚ doporučuje, aby toto sdělení bylo učiněno primárně elektronicky (e-mailem či datovou schránkou) a aby obsahovalo identifikaci správce či zpracovatele, taktéž pověřence (jméno a příjmení) a kontaktní údaje pověřence (e-mailová adresa a telefonní číslo).[361]

Pověřenec je aktivně zapojen také do procesu předchozí konzultace dle čl. 36 GDPR. Nad rámec toho pověřenec může s dozorovým úřadem konzultovat různé problémy související s ochranou osobních údajů, k čemuž by ÚOOÚ pověřenci měl vždy poskytnout relevantní stanovisko.

359 Čl. 39 odst. 1 písm. d) a e) GDPR.

360 WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, op. cit.

361 ÚOOÚ: *Pověřenci: Nejdůležitější informace a nejčastější dotazy k pověřenci pro ochranu osobních údajů (DPO)*. Dostupné na https://www.uoou.cz/k-poverenci-pro-ochranu-osobnich-udaju-dpo/ds-5005.

Závěr

Tato diplomová práce se věnovala vcelku aktuálnímu tématu ochrany osobních údajů, jež se dotýká též zaměstnavatele jako správce, který zpracovává značné množství osobních údajů zaměstnanců, a to jak za trvání pracovněprávního vztahu, tak i před jeho vznikem či po jeho zániku. Zaměstnavatelé by tak, stejně jako jiní správci osobních údajů, měli dbát o to, aby při zpracování osobních údajů svých zaměstnanců dodrželi veškeré požadavky určené právními předpisy na ochranu osobních údajů.

Hlavním zdrojem právní úpravy ochrany osobních údajů je v prostředí EU dnes GDPR, tedy nařízení EU, které nabylo účinnosti dne 25. 5. 2018. V návaznosti na účinnost GDPR pak jednotlivé členské státy přijímaly právní předpisy adaptující vnitrostátní právní řad na účinnost GDPR. GDPR si klade ambice stát se právním předpisem, který sjednotí rámec ochrany osobních údajů v EU, což potvrzuje i druh zvoleného právního aktu, tedy nařízení, jež je přímo aplikovatelné ve všech členských státech EU. Zůstává však s otazníkem, zda se podaří tohoto cíle plně dosáhnout, a to zejména s ohledem na skutečnost, že rozhodovací praxe a výklad GDPR ze strany národních dozorových úřadů se může do určité míry lišit. Určité rozdíly v úpravě ochrany osobních údajů napříč členskými státy EU mohou pramenit též z různých znění adaptačních zákonů přijímaných v souvislosti s účinností GDPR. Až čas tedy napoví, zda bude naplněn cíl sjednocení právní úpravy ochrany osobních údajů.

Cílem této diplomové práce nebylo poskytnout komplexní analýzu práv či povinností vztahujících se dle GDPR na správce osobních údajů. Vzhledem k obsáhlosti tohoto tématu by ani nebylo možné v rámci diplomové práce toto v celé šíři postihnout. Cílem práce bylo spíše věnovat se konkrétněji některým vybraným aspektům a povinnostem vztahujícím se na správce osobních údajů. Zároveň však autorka považovala za vhodné zařadit do práce pojednání o historickém kontextu právní úpravy ochrany osobních údajů, a to zejména s důrazem na přijetí nového evropského rámce právní úpravy ochrany osobních údajů, jehož součástí bylo i přijetí GDPR. Do diplomové práce je zařazen i přehled základních pojmů z oblasti zpracování osobních údajů uvedených v GDPR, se kterými je pracováno též v této diplomové práci a jejichž výklad autorka považovala za podstatný v kontextu obsahu této práce.

Podstatná část diplomové práce je věnována samotným povinnostem, které se na správce vztahují, počínaje základními zásadami zpracování osobních údajů, kterými se

správce při zpracování osobních údajů musí řídit a dále jsou blíže rozebrány vybrané povinnosti správce, které nově přineslo GDPR.

Účinnost GDPR přinesla jisté změny v oblasti zpracování osobních údajů, které, dle názoru autorky, sice nejsou tak rozsáhlé, jak bývají širší veřejností někdy vnímány, nicméně správci museli tyto změny reflektovat a ideálně provést posouzení, zda dosavadní mechanismy související se zpracováním osobních údajů odpovídají požadavkům kladeným GDPR. Na pozoru by měli být zejména správci provádějící rozsáhlé či rizikové zpracování osobních údajů, jelikož na mnohé z nich se budou vztahovat některé z nových povinností.

Za jednu z podstatnějším změn zakotvenou GDPR bývá označováno posílení principu odpovědnosti správce, a to v tom smyslu, že v GDPR je nově výslovně uvedena povinnost správce doložit soulad jím prováděného zpracování s GDPR. Nově je též rozšířen princip založený na riziku. S rozšířením principu založeného na riziku a zdůrazněním principu odpovědnosti správce souvisí též některé nové dodatečné povinnosti vztahující se typicky na správce provádějící zpracování, jenž představuje riziko či vysoké riziko pro subjekty údajů.

K těmto povinnostem se řadí také povinnost vést záznamy o činnostech zpracování, povinnost jmenovat pověřence na ochranu osobních údajů či provádět posouzení vlivu na ochranu osobních údajů. Právě důkladnějšímu rozboru těchto tří povinností je věnována poslední kapitola diplomové práce.

Autorka považuje posílení principu odpovědnosti správce a rozšíření přístupu založeného na riziku v zásadě za pozitivní tendenci v oblasti ochrany osobních údajů, jelikož subjekty údajů jsou, zvlášť s ohledem na neustávající rozvoj technologií, stále více zranitelní. Po roce od účinnosti GDPR však zatím nejsou úplně sjednoceny např. názory ohledně toho, jakým způsobem a na koho se budou vztahovat výše nastíněné dodatečné povinnosti dopadající na skupiny správců provádějící zpravidla více rizikové zpracování z pohledu subjektů údajů. K dnešnímu dni tedy, dle názoru autorky, mezi správci stále může panovat nejistota ohledně toho, zda a v jakém rozsahu se na ně budou vztahovat tyto dodatečné povinnosti, což souvisí též s tím, že i mezi odborníky věnujícími se právu na ochranu osobních údajů se mohou názory na výklad takových povinností různit. Ke sjednocení výkladu by měly přispět zejména národní dozorové úřady, ať už rozhodovací praxí, nebo stanovisky, stejně jako Sbor.

Co se týče obecného zhodnocení přijetí GDPR zejména z praktického hlediska, autorka je toho názoru, že přijetí GDPR mnoho správců motivovalo k tomu, aby

zrevidovali mechanismy jimi prováděného zpracování osobních údajů a zaměřili se na dosažení souladu s předpisy na ochranu osobních údajů, což lze hodnotit pozitivně. Autorka též kladně hodnotí rozšíření či zpřesnění projevů zásady transparentnosti, tedy např. bližší rozvedení požadovaného rozsahu informací, které je povinen správce sdělit subjektu údajů v okamžiku získání osobních údajů, nebo rozšíření výčtu práv subjektů údajů. Co se týče negativ, autorka v zásadě souhlasí s názorem, že GDPR může přinést větší administrativní a/nebo finanční náročnost pro správce, a to zejména s ohledem na plnění tzv. dodatečných povinností.

Seznam zkratek

Směrnice 95/46/ES	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
ZOOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
ÚOOÚ	Úřad pro ochranu osobních údajů
WP29	Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená dle čl. 29 Směrnice 95/46/ES (v angličtině Article 29 Data Protection Working Party)
Sbor	Evropský sbor pro ochranu osobních údajů zřízený dle čl. 68 GDPR (v angličtině European Data Protection Board)
SDEU	Soudní dvůr Evropské unie
ZZOÚ	Vládní návrh zákona o zpracování osobních údajů
Evropská úmluva	Úmluva o ochraně lidských práv a základních svobod
EU	Evropská unie
LZPS	Listina základních práv a svobod
Evropská Komise	Komise

Zákoník práce	Zákon č. 262/2006 Sb., zákoník práce
OZ	Zákon č. 89/2012 Sb., občanský zákoník

Seznam použitých zdrojů

Právní předpisy

Právní předpisy ČR

Zákon č. 262/2006 Sb., zákoník práce

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

Zákon č. 435/2004 Sb., o zaměstnanosti

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon)

Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení

Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění

Zákon č. 187/2006 Sb., o nemocenském pojištění

Zákon č. 586/1992 Sb., o daních z příjmů

Vládní návrh zákona o zpracování osobních údajů, sněmovní tisk 138/0

Zákon č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru

Právní předpisy EU

Smlouva o fungování EU

Listina základních práv EU

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

Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV („trestněprávní směrnice o ochraně osobních údajů“)

Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti

Mezinárodní dokumenty

Všeobecná deklarace lidských práv

Mezinárodní pakt o občanských a politických právech

Úmluva o ochraně lidských práv a základních svobod

Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. 1. 1981

Judikatura

Rozsudek Soudního dvora ze dne 31. ledna 1978 ve věci 94/77, *Fratelli Zerbone Snc v. Amministrazione delle finanze dello Stato*

Rozsudek SDEU ze dne 19. října 2016 ve věci C-582/14, *Patrick Breyer proti Spolkové republice Německo*

Rozsudek SDEU ze dne 6. listopadu 2003 ve věci C-101/01, *Bodil Lindqvist proti Švédsku*

Rozsudek SDEU ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Hessensku*

Rozsudek Soudního dvora ve věci 6/64, *Flaminio Costa vs. E.N.E.L*

Rozsudek SDEU ze dne 13. května 2014 ve věci C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*

Rozsudek SDEU ze dne 25. listopadu 2011 ve věci C-468/10, *Asociación Nacional de Establecimientos Financieros de Crédito v. Administración del Estado*

Rozsudek SDEU ze dne 4. května 2017 ve věci C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas Satiksme“*

Rozsudek Evropského soudu pro lidská práva ze dne 16. prosince 1992 ve věci stížnosti č. 13710/88, *Niemietz v. Německo*

Rozsudek Evropského soudu pro lidská práva ze dne 12. ledna 2016 ve věci stížnosti č. 61496/08, *Barbulescu v. Rumunsko*

Nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94

Nález Ústavního soudu ze dne 9. 3. 2004, sp. zn. Pl. ÚS 38/02

Nález Ústavního soudu ze dne 10. 11. 1998, sp. zn. I. ÚS 229/98

Rozsudek Nejvyššího správního soudu ze dne 5. 11. 2009, sp. zn. 1 Afs 60/2009

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

Odborná literatura

NAVRÁTIL, J. a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, ISBN 978-80-7380-689-7

ŽŮREK, J. *Praktický průvodce GDPR*, Praha: ANAG, 2017, ISBN 978-80-7554-097-3

MAŠTALKA, J. *Osobní údaje, právo a my. 1. vydání*. Praha: C. H. Beck, 2008, ISBN 978-80-7400-033-1

MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. *1. vydání.* Praha: Wolters Kluwer, 2013, ISBN 978-80-7478-139-1

PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kol., *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. Praha: Leges, 2018, ISBN 978-80-7502-288-2

NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR, 2017, ISBN 978-80-7552-765-3

KUČEROVÁ, A., NOVÁKOVÁ L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář. 1.* vydání. Praha: C. H. Beck, 2012, ISBN 978-80-7179-226-0

BARTÍK V., JANEČKOVÁ E.: *Zákon o ochraně osobních údajů s komentářem*. Olomouc: ANAG, 2010, ISBN 978-80-7263-613-6

POLČÁK, R. a kol. *Právo informačních* technologií. Praha: Wolters Kluwer ČR, 2018, ISBN 978-80-7598-045-8

BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář. 2. vydání*. Praha: C. H. Beck, 2015, ISBN 978-80-7400-290-8

PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, ISBN 978-80-7552-609-0

BARTÍK V., JANEČKOVÁ E. *Ochrana osobních údajů z pohledu zvláštních právních úprav k 1. 8. 2012*. 1. vydání. Olomouc: ANAG, 2012, ISBN 978-80-7263-749-2

BARTÍK V., JANEČKOVÁ E. *Ochrana osobních údajů v aplikační praxi (vybrané problémy). 4. vydání*. Praha: Wolters Kluwer ČR, 2016, ISBN 978-80-7552-141-5

BĚLINA M. a kol. *Pracovní právo, 6. vydání*, Praha: C. H. Beck, 2014

BĚLINA, M., PICHRT, J. a kol. *Pracovní právo. 7. doplněné a podstatně přepracované vydání*. Praha: C. H. Beck, 2017, ISBN 978-80-7400-283-0

JANEČKOVÁ, E., *GDPR. Praktická příručka implementace*. Praha: Wolters Kluwer ČR, a.s., 2018, ISBN 978-80-7552-248-1

NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: GRADA Publishing, a.s., 2018, ISBN 978-80-271-0668-4

GDPR v kostce: praktický průvodce povinnostmi pro podniky a spolky. Praha: C. H. Beck, 2018. ISBN 978-80-7400-704-0

DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M. a kol. *Občanské právo hmotné*. *Svazek 1. Díl první: Obecná část.* Praha: Wolters Kluwer ČR, 2013, s. 357-359. ISBN 978-80-7478-325-8

LAVICKÝ, P. *a kol.: Občanský zákoník I. Obecná část (§ 1−654). Komentář*. 1. vydání, Praha: C. H. Beck, 2014, ISBN 978-80-7400-529-9

Články

České

ZEMANOVÁ ŠIMONOVÁ, H. *Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů*. Bulletin advokacie 9/2017, s. 25

MORÁVEK, J. *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy 13-14/2018

MAŠTALKA, J. *Nové nařízení EU o ochraně osobních údajů a některé záležitosti spojené s jeho aplikací v ČR*. Právní rozhledy 21/2016

MATEJKA, J., KRAUSOVÁ, A., GÜTTLER, V., *Biometrické údaje a jejich právní režim*. Revue pro právo a technologie 17/2018

JANEČKOVÁ, E., BARTÍK, V. *Osobní spis zaměstnance jako zpracování osobních údajů,* Práce a mzda 2009/7

MORÁVEK, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*, Právní rozhledy 17/2017

NONNEMANN, F. *Soukromí na pracovišti*, Právní rozhledy 7/2015

ZEMANOVÁ ŠIMONOVÁ, H. *Právní prostředky ochrany osobnosti zaměstnance.* Bulletin advokacie. 10/2016

MATYSOVÁ, M., NONNEMANN, F., *Možnost odmítnout uplatnění práva subjektu údajů dle GDPR.* Právní rozhledy 12/2018

NONNEMANN, F. *Aktuální judikatura SDEU k oprávněnému zájmu jako právnímu titulu pro zpracování osobních údajů*. Právní rozhledy 15-16/2017, s. 541

MALIŠ, P. *GDPR - 3. díl: Vedení záznamů o činnostech zpracování osobních údajů*. IT Systems č. 10/2017, dostupné na http://www.pravoit.cz/novinka/gdpr-3-dil-vedeni-zaznamu-o-cinnostech-zpracovani-osobnich-udaju

OTEVŘEL P., *GDPR - 4. díl: Jste povinni jmenovat pověřence pro ochranu osobních údajů?* IT Systems č. 11/2017, dostupné na http://www.pravoit.cz/novinka/gdpr-4-dil-jste-povinni-jmenovat-poverence-pro-ochranu-osobnich-udaju.

NEŠPŮREK R., ŠUCHMAN J., JAROŠ J. *Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?* 26. 3. 2018. Dostupné na https://www.epravo.cz/top/clanky/poverenec-pro-osobni-udaje-dle-gdpr-kdy-koho-a-jak-poverit-107265.html

NEŠPŮREK, R., ŠUCHMAN, J., JAROŠ, J. *GDPR: Kdy a jak posuzovat vliv zpracování na ochranu osobních údajů a kdy konzultovat dozorový orgán?* 9. 11. 2017. Dostupné na https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/gdpr-kdy-a-jak-posuzovat-vliv-zpracovani-na-ochranu-osobnich-udaju-a-kdy-konzultovat-dozorovy-organ

Vláda: ÚOOÚ: Stanovisko k povinnosti provádět posouzení vlivu na ochranu osobních údajů. Právní rozhledy 13-14/2018, s. 3

Zahraniční

KISS, A., SZÖKE, G. L. *Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation.* In GUTWIRTH, S., LEENES, R., DE HERT, P. (eds.). *Reforming European Data Protection Law.* 20. vyd. Heidelberg: Springer, 2015, Law Governance and Technology Series

VAN EIJK, N. *About Finding Practical Solutions (Without the GDPR)*. European Data Protection Law Review, Vol. 3, Issues 3 (2017)

The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. Dostupné na https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

MACENAITE M., KOSTA E. *Consent for processing children's personal data in the EU: following in US footsteps?* Information & Communications Technology Law

DETLEV, G., HICKMAN, T., *Chapter 6: Data Protecting Principles – Unlocking the EU General Data Protection Regulation*, 22. 7. 2016. Dostupné na

https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection

DETLEV, G., HICKMAN, T., *Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation*. 13. 9. 2017. Dostupné na https://www.whitecase.com/publications/article/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data

VOIGT, P., *The compliance burden under the GDPR – Data Protection Officers*. Září 2016. Dostupné na https://globaldatahub.taylorwessing.com/article/the-compliance-burden-under-the-gdpr-data-protection-officers

BOND, R., *The Role of the Data Protection Officer In Europe*. 6. 10. 2015. Dostupné na https://s3.amazonaws.com/documents.lexology.com/1373a119-14ae-4732-aed4-d9fbec519dc8.pdf

KAUFMANN, J., GUENTHER, J. *Germany: Data Protection Officer must not have a conflict of interests*. 21. 11. 2016. Dostupné na https://globalcompliancenews.com/germany-data-protection-officer-conflict-of-interest-20161121/

KAUFMANN, J., GUENTHER, J. *Data Protection Officers Must Not Have a Conflict of Interest – Part 2*. 9. 1. 2018. Dostupné na https://globalcompliancenews.com/data-protection-officers-conflict-interest-20180109/

BIEKER, F., FRIEDEWALD, M., HANSEN, M., OBERSTELLER, H., ROST, M. *A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation*. Springer International Publishing Switzerland 2016

YORDANOV, A. *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation, European Data Protection Law Review*, 4/2017, s. 486-495

Další prameny

Sdělení Komise Evropskému parlamentu a Radě ze dne 16. 8. 2018, COM(2018) 43 final/2, dostupné na http://ec.europa.eu/transparency/regdoc/rep/1/2018/CS/COM-2018-43-F2-CS-MAIN-PART-1.PDF

Sdělení ÚOOÚ *Nové přístupy a povinnosti*, dostupné na https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=4720

Endorsement of GDPR WP29 Guidelines (Endorsement 1/2018) dostupné na https://edpb.europa.eu/node/89

Dokument ÚOOÚ Desatero omylů, dostupné na https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=4818&n=desatero-omylu&p1=3938
Dokument ÚOOÚ *Základní příručka k GDPR, 2. Nové přístupy a povinnosti*. Dostupné na https://www.uoou.cz/2-nove-p-istupy-a-povinnosti/d-27268

Důvodová zpráva k vládnímu návrhu zákona o zpracování osobních údajů

Tisková zpráva ÚOOÚ ze dne 31. srpna 2018. *Sdělení předsedkyně Úřadu k vyžadování souhlasu*. Dostupné na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31695

Information Commissioner's Office. *Consultation: GDPR consent guidance*. Dostupné na https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Rada Evropy, *doporučení Výboru ministrů Rady Evropy členským státům č. CM/Rec (2015) ohledně zpracování osobních údajů v souvislosti se zaměstnáním*, odstavec 13.2. Dostupné na https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

ÚOOÚ: Základní příručka k GDPR, 6. Práva subjektu údajů, dostupné na https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

ÚOOÚ *K problematice aktualizace zpracovávaných osobních údajů*. Dostupné na https://www.uoou.cz/k-problematice-aktualizace-zpracovavanych-osobnich-udaju/d-1595

Zpravodajství Ministerstva vnitra ČR, Vitnerová, M., *Vláda schválila návrh zákona o zpracování osobních údajů*. Dostupné na https://www.mvcr.cz/clanek/vlada-schvalila-navrh-zakona-o-zpracovani-osobnich-udaju.aspx

ÚOOÚ: Základní příručka k GDPR, 9. Pověřenec pro ochranu osobních údajů. Dostupné na https://www.uoou.cz/9-poverenec-pro-ochranu-osobnich-udaju/d-27280

Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí podle právního stavu k 10. srpnu 2017. Dostupné na https://www.mvcr.cz/clanek/zpravodajstvi-institut-poverence-pro-ochranu-osobnich-udaju-informace-pro-obce.aspx

ÚOOÚ: *Pověřenci: Nejdůležitější informace a nejčastější dotazy k pověřenci pro ochranu osobních údajů (DPO)*. Dostupné na https://www.uoou.cz/k-poverenci-pro-ochranu-osobnich-udaju-dpo/ds-5005

Důvodová zpráva k zákonu č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru

Information Commissioner's Office: Privacy Impact Assessment Executive Summary. Dostupné na https://ico.org.uk/media/about-the-ico/consultations/2047/pia-executive-summary.pdf

Dokument ÚOOÚ *K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA)*. Dostupný na https://www.uoou.cz/k-nbsp-povinnosti-spravcu-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju/d-33194

Návrh dokumentu ÚOOÚ *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)*. Dostupné na https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385

ÚOOÚ: *Návrh seznamu operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů*. Dostupné na https://www.uoou.cz/dokumenty-k-gdpr/ds-4720/p1=4720

Stanoviska/Pokyny WP29 a Sboru

WP29: Stanovisko č. 4/2007, *k pojmu osobní údaj*

Working Party document No WP 105: "*Working document on data protection issues related to RFID technology*", přijatý dne 19. 1. 2005

WP29: *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*, přijaté dne 3. října 2017, ve znění naposledy revidovaném a přijatém dne 6. února 2018

WP29: Stanovisko č. 1/2010 *k pojmům „správce" a „zpracovatel"*, přijaté dne 16. února 2010

WP29: Stanovisko č. 15/2011 *o definici souhlasu*, přijaté dne 13. července 2011

WP29: *Pokyny pro souhlas podle nařízení 2016/679*, přijaté dne 28. listopadu 2017, v revidovaném znění přijatém dne 10. dubna 2018

WP29 Stanovisko č. 2/2017, *ke zpracování údajů na pracovišti* přijaté dne 8. června 2017

WP29: Stanovisko č. 06/2014 *ke konceptu oprávněného zájmu dle čl. 7 Směrnice 95/46/ES*, přijaté dne 9. dubna 2014

WP29: *Pokyny k transparentnosti podle nařízení 2016/679*, přijaty dne 29. listopadu 2017, ve znění naposledy revidovaném a přijatém dne 11. dubna 2018

WP29: Stanovisko č. 3/2013 *k účelovému omezení*, přijaté dne 2. dubna 2013

WP29: Stanovisko č. 3/2010 *k zásadě odpovědnosti*, přijaté dne 13. července 2010

WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*, přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017

WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679WP29*, přijaté dne 4. 4. 2017, v aktualizovaném znění přijaté dne 4. 10. 2017

Opinion of the Board (Art. 64) 4/2018 on the draft list of the competent supervisory authority of Czech Republic regarding the processing operations subject to the

requirement of a data protection impact assessment (Article 35.4 GDPR). Adopted on 25th September 2018. Dostupné na https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

Stanoviska ÚOOÚ

ÚOOÚ: Stanovisko č. 6/2012, *Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů*

ÚOOÚ: Stanovisko č. 2/2001, *Zpracování citlivého osobního údaje o členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací*

ÚOOÚ: Stanovisko č. 4/2012, *Zpracování osobních údajů zemřelých osob*

ÚOOÚ: Stanovisko č. 2/2009 *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*

ÚOOÚ: Stanovisko č. 1/2006 *Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*

ÚOOÚ: Stanovisko č. 3/2014 *K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti*

Abstrakt

Diplomová práce se věnuje aktuálnímu tématu ochrany osobních údajů se zaměřením na povinnosti správce, které se ve velké míře vztahují též na zaměstnavatele jakožto správce osobních údajů zaměstnanců. Diplomová práce vychází primárně z právní úpravy ochrany osobních údajů obsažené v GDPR s tím, že v některých pasážích je obsažena komparace s dříve účinnými právními předpisy na ochranu osobních údajů. Cílem práce je poskytnout ucelený přehled základních institutů ochrany osobních údajů z pohledu správce se zaměřením na analýzu některých povinností, které nově přineslo GDPR.

Diplomová práce je rozdělena na čtyři kapitoly, které jsou dále členěny na poměrně značné množství podkapitol. První kapitola je věnována historickému přehledu právní úpravy na ochranu osobních údajů, a to jak na úrovni mezinárodní, tak na úrovni Evropy (Evropské unie) a národní.

Druhá kapitola práce obsahuje bližší vymezení základních pojmů souvisejících s právní úpravou ochrany osobních údajů, se kterými operuje GDPR, jako je pojem osobní údaj, subjekt údajů, správce a zpracovatel, příjemce či zpracování osobních údajů.

Třetí kapitola se zabývá základními zásadami ovládajícími zpracování osobních údajů, tedy zcela zásadními povinnostmi, kterými se musí správci i zpracovatelé při zpracování osobních údajů řídit. Detailně jsou zde rozebrány zejména zásady zákonnosti, korektnosti či transparentnosti. Do této kapitoly je začleněna i analýza právních důvodů pro zpracování osobních údajů taxativně vyčtených v GDPR.

Poslední kapitola pak blíže pojednává o vybraných povinnostech správce osobních údajů. Jedná se o povinnosti, které je v rámci českého prostředí možné označit v zásadě za nové. Poukázáno je zde i na určité nejasnosti související s aplikací těchto povinností v praxi.

V závěru práce je pak stručně shrnut obsah diplomové práce a závěry v ní obsažené.

Klíčová slova

Ochrana osobních údajů, povinnosti správce osobních údajů, GDPR

Abstract

This diploma thesis deals with the topic of personal data protection, and focuses particularly on the duties of the data controller, which also largely apply to the employer as the controller of the personal data of the employees. The diploma thesis builds primarily on the legal regulation of personal data protection contained in GDPR, while in some sections, a comparison with the previously effective personal data protection legislation is included. The objective of this diploma thesis is to provide a comprehensive overview of fundamental personal data protection institutes from the data controller's point of view with a focus on the analysis of some of the obligations which has been newly introduced by GDPR.

The diploma thesis is divided into four chapters, which are further divided into a relatively high number of subchapters. The first chapter contains a historical overview of legislation on personal data protection at the international and European (European Union) level as well as national levels.

The second chapter defines the fundamental terms related to personal data protection which are used in GDPR, such as personal data, data subject, data controller and processor, recipient of the personal data or personal data processing.

The third chapter discusses the fundamental principles relating to processing of personal data, that is, the fundamental obligations that controllers and processors must observe when processing personal data. In particular, the principles of lawfulness, fairness and transparency are discussed in detail. This chapter also includes an analysis of legal grounds for the processing of personal data which are exhaustively listed in GDPR.

The last chapter deals with some of the specific duties of data controllers. These are the obligations that may be classified as new within the Czech legal order. Some confusion related to the application of these obligations in practice is also highlighted in this chapter.

The conclusion of the diploma thesis summarizes the content of the thesis and the findings included in it.

Keywords

Personal data protection, duties of the data controller, GDPR